Timo Summa

Syvyyssuuntainen puolustus – Suurin uhka tulee sisältä

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

TXK20S2

Insinöörityö

11.4.2021

Tiivistelmä

Tekijä:	Timo Summa
Otsikko:	Syvyyssuuntainen puolustus – Suurin uhka tulee sisältä
Sivumäärä:	51 sivua
Aika:	11.4.2021
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	TXK20S2
Ammatillinen pääaine:	Tietoverkot
Ohjaajat:	Janne Salonen, Opettaja

Syvyyssuuntainen puolustus (Security in Depth) on suojausmenetelmä, jolla yritys voi vähentää yrityksen toimintaan kohdistuvia turvallisuusriskejä. Tämän tutkielman tarkoituksena on selvittää yrityksen syvyyssuuntaista puolustusta suunniteltaessa huomioon otettavia asiakokonaisuuksia.
Tutkielmassa tarkastellaan keskeiset turvajärjestelyjen osa-alueet, joilla on merkitys yrityksen syvyyssuuntaisen puolustuksen kokonaisuuteen, ja annetaan aihealueittain suosituksia keskeisten asioiden huomioimiseksi suunniteltaessa ja kehitettäessä yrityksen turvajärjestelmää.
Tutkielma käsittelee turvajärjestelyjen (Security) näkökulmasta syvyyssuuntaista puolustusta. Tutkielmassa haetaan kirjallisuusselvityksen menettelyin vastauksia, miten turvajärjestelyjen hallinto, yrityksen fyysinen ympäristö, tekniset valvontajärjestelmät ja turvaorganisaatio vaikuttavat syvyyssuuntaisen puolustuksen muodostumiseen. Tutkielmakysymyksiin haetaan vastauksia International Atomic Energy Agencyn (IAEA) laatimista ohjeista, Säteilyturvakeskuksen (STUK) määräyksistä ja ohjeista sekä aihealueeseen liittyvistä tutkimusmateriaaleista ja julkaisuista.
Aihealuetta tarkasteltaessa käsiteltyä aineistoa on sovellettu yleistäen sitä, jotta se soveltuisi käytettäväksi laajemmin yritysmaailman käyttöön. Tarkastelun kohteena oleva lähdedokumentaatio on pääosin tarkoitettu ydinlaitosten turvallisuuden varmistamiseen, mutta sen perusteella esitetyt menettelyt voidaan soveltaa kaikille toimialoille ja kaikkiin yrityksiin.
Tutkielman tuloksena havaittiin, että tehokkaan syvyyssuuntaisen puolustuksen rakentaminen edellyttää koko organisaation osallistumista turvajärjestelyjen toteuttamiseen ja turvallisuusajattelun muodostumiseen yrityksessä. Turvajärjestelyt muodostuvat hyvin järjestetystä hallinnollisesta, fyysisestä, teknisestä ja operatiivisesta toiminnallisesta kokonaisuudesta. Erityisesti sisäiset Insider-uhat muodostavat vaikeusasteen turvajärjestelyjen toteuttamiselle siitä syystä, että Insider voi toimia yrityksessä missä tahansa tehtävässä ja voi aiheuttaa uhan millä tahansa syvyyssuuntaisen puolustuksen vyöhykkeillä.

Avainsanat: Syvyyssuuntainen puolustus, DiD, SiD, turvavyöhyke, vartiosto, turvallisuus, riski, uhka, turvajärjestelyt, IAEA, STUK

Abstract

Author:	Timo Summa
Title:	Security in Depth - The biggest threat comes from the inside.
Number of Pages:	51 pages
Date:	11 April 2021
Degree:	Bachelor of Engineering
Degree Programme:	TXK20S2
Professional Major:	Iot & Cloud Computing
Instructors:	Janne Salonen, Principal Lecturer

Security in Depth is a security method by which a company can reduce the security risks to its operations. The purpose of this study is to find out the issues to be considered when planning a company's Security in Depth practices.
The study examines the key aspects of security arrangements that are relevant to the company's Security in Depth defence as a whole and makes thematic recommendations for taking key issues into account when designing and developing a company's security system.
The study deals with Security in Depth from the point of view of security arrangements. The study seeks answers through the literature review procedures on how the management of security arrangements, the physical environment of the company, technical security control systems and the security organization affect the formation of Security in Depth defence. Answers to the study questions are sought from the guidelines prepared by the International Atomic Energy Agency (IAEA), the regulations and guidelines of the Finnish Radiation and Nuclear Safety Authority (STUK), and research materials and publications related to the topic.
When considering the topic, the material discussed has been applied in a general way in order to make it more suitable for use in the business world. The source documentation under review is mainly intended to ensure the safety of nuclear installations and sites, but the practices presented can be applied to all industries and all companies.
As a result of the study, to building an effective Security in Depth defence requires the participation of the entire organization in the implementation of security arrangements and the formation of security culture in the company. Security arrangements consist of a well-organized administrative, physical, technical and operational functional entity. Insider’s threats pose a difficulty in implementing security arrangements, because Insider can operate in any position in the company and can pose a threat in deep in defence zones.

Keywords: Defence in Depth, DiD, SiD, Security zone, Guarding, Security in Depth, Security, Risk, Threat, Security arrangements, IAEA, STUK

Sisällys

Termit ja lyhenteet

Ennalta ehkäisevä toimenpide: Termiä käytetään kuvaamaan toimenpiteitä, joilla voidaan vaikuttaa uhan muodostumiseen.

IAEA: International Atomic Energy Agency. Kansainvälinen järjestö, jonka tavoitteena on edistää ydinteknologian turvallista, turvallista ja rauhanomaista käyttöä.

Insider: Sisäinen uhka. On henkilö tai taho, jolla on mahdollisuus vaikuttaa yrityksestä sisältäpäin uhan muodostamiseen.

Outsider: Ulkoinen uhka. On yrityksen ulkopuolinen henkilö tai taho, joka pyrkii toteuttamaan uhan tunkeutumalla yritykseen tai vaikuttamalla yrityksen toimintaan.

Regulaatio: On sääntelyä, jota käytettään jonkin toimialan ohjaamiseen.

STUK: Säteilyturvakeskus. On sosiaali- ja terveysministeriön hallinnonalan viranomainen, joka valvoo säteily- ja ydinturvallisuutta Suomessa.

Suojattava kohde: Asset. On suojattava arvo, joka voi olla aineellinen tai aineeton ja jolla on merkittävä arvo haltijalle.

Suunnitteluperusteuhka: Design Basis Threat. DBT. On menetelmä, jolla turvajärjestelyjen suunnitteluperuste johdetaan uhkakuvasta ja lainvastaisen tai muun ydin- tai säteilyturvallisuutta vaarantavan toiminnan mahdollisista seurauksista

Syvyyssuuntainen puolustus: Defence in Depth. DiD. Security in Depth. SiD. On useiden järjestelmien ja toimenpiteiden yhdistelmä, jotka uhan aiheuttajan on voitettava tai kierrettävä ennen kuin suojattava arvo tai omaisuus vaarantuu. Turvajärjestelyjen yhteydessä käytetään englanninkielistä termiä Security in Depth.

Turvavyöhyke: Security zone. On fyysinen tai looginen alue, joka halutaan suojata luvattomalta pääsyltä.

Uhka: Threat. On käsite, jolla voidaan aiheuttaa vahinkoa ihmisille, omaisuudelle tai ympäristölle.

Uhan aiheuttaja: Adversary. Käsitettä käytetään kaikista tahoista/henkilöistä, jolla on kyky toteuttaa tahallinen (Malicious) teko. Uhan aiheuttaja on Insider tai Outsider tai ne yhdessä.

Uhkaskenaario: On suunnittelun perustaksi luotu kuvaus määritellyn uhan mahdollisesta toteuttamistavasta.

1 Johdanto

Tämän tutkielman tarkoituksena on selvittää yrityksen tai organisaation syvyyssuuntaista puolustusta suunniteltaessa asiakokonaisuuksia, jotka on otettava huomioon turvajärjestelyissä. Syvyyssuuntainen puolustus on suojausmenetelmä, jolla yritys voi vähentää yrityksen toimintaan kohdistuvia turvallisuusriskejä.

Tutkielman tulokset ovat merkityksellisiä, kun yritys suunnittelee tai kehittää omaa turvajärjestelmäänsä ja tarvitsee suunnittelunsa tueksi kuvaukset keskeisistä turvajärjestelmän kehittämisalueista. Tutkielmassa tarkastellaan turvajärjestelyjen eri asiakokonaisuuksia periaatetasolla. Teoreettisen lähestymistavan lisäksi tutkielmassa esitetään esimerkki missä laajuudessa yrityksessä voi soveltaa tutkielman tuloksia.

Tutkimuksessa haetaan vastauksia seuraaviin kysymyksiin:

- Miten hallinto ja johtaminen tulee ottaa huomioon turvallisuuden kehittämisessä.
- Miten varautua uhkiin ja miten niitä voidaan hallita.
- Miten fyysinen ympäristö vaikuttaa turvallisuuteen.
- Miten teknisillä järjestelmillä voidaan tukea turvallisuustoimintaa.
- Miten operatiivinen toiminta liittyy turvallisuuden muodostumiseen.

Tutkielmakysymyksiin haetaan vastauksia International Atomic Energy Agencyn (IAEA) laatimista ohjeista, Säteilyturvakeskuksen (STUK) määräyksistä ja ohjeista sekä aihealueeseen liittyvistä tutkimusmateriaaleista ja julkaisuista. Tarkastelun kohteena oleva dokumentaatio on pääosin tarkoitettu ydinlaitosten turvallisuuden varmistamiseen, mutta sitä voidaan soveltaa kaikille toimialoille ja kaikkiin yrityksiin.

IAEA on ohjeistuksessaan suositellut turvajärjestelyjen suunnitteluun käytettäväksi suunnitteluperusteuhkaa. Ydinvoima-alalla IAEA on velvoittanut eri valtiot

määrittelemään kansalliset kriteerit uhkien torjuntaan. Nämä kriteerit on kuvattu suunnitteluperusteuhkaan (Design Basis Threat). Suunnitteluperusteuhka määrittelee ne uhkaskenaariot, joita vastaan ydinvoimalaitoksessa on turvallisuuteen liittyvät järjestelmät suunniteltava. IAEA:n ohjeistus, ja kansallinen suunnitteluperusteuhka antavat hyvän viitekehyksen suunnitella myös muiden toimialojen kuin ydinvoima-alan turvajärjestelyjä. Tämän takia yritykset, joilla ei ole regulaation määrittelemää suunnitteluperusteuhkaa, tulisi itse laatia uhkaskenaariot, joita vastaan liiketoiminta tulisi suojata.

Käytettyjen lähdeaineistojen tietoja on tässä tutkielmassa sovellettu turvallisuuskriittisten yritysten näkökulmasta. Tekstissä on pyritty hävittämään myös suorat liitokset ydinvoimateknologiaan ja sen erityisvaatimuksiin.

Tämän tutkielman tarkoituksena on selvittää, millaisista osakokonaisuuksista syvyyssuuntaisen puolustuksen suojausmenetelmä koostuu ja millaisia näkökulmia osakokonaisuuksien toteutuksessa yrityksen tulisi huomioida.

Syvyyssuuntainen puolustus on suojausmenetelmä, jota voidaan käyttää henkilöiden tai omaisuuden suojaamiseen. Menetelmällä pyritään estämään omaisuuteen kohdistuva uhka tai pienentämään uhan vaikutusta. Oleellista menetelmässä on suojauksen kerroksellisuus, jota käytetään uhan havaitsemiseen, estämiseen ja viivästyttämiseen.

Syvyyssuuntaisen puolustuksen lähtökohtana on hyvä johtamis- ja turvallisuuskulttuuri. Koko yrityksen henkilöstön on noudatettava turvallisuudesta annettuja määräyksiä ja ohjeistusta. Kaikkiin poikkeamiin määritellyistä suojaustoimenpiteistä on reagoitava ja arvioitava poikkeamien vaikutus turvallisuuteen. Ihmiset ja inhimillinen käytös kuitenkin ovat viimekädessä tekijät, jotka määrittelevät syvyyssuuntaisen puolustuksen vaikuttavuuden.

Suunniteltaessa syvyyssuuntaista puolustusta on tunnistettava kriittiset toiminnot tai omaisuus, eli suojattavat kohteet. Suojattavan kohteen määrittely tapahtuu esimerkiksi kohteen rahallisen arvon, sen merkityksen liiketoiminnalle tai tiedon arkaluonteisuuden perusteella.

Syvyyssuuntaista puolustusta suunniteltaessa on oleellista tunnistaa suojattavaa kohdetta mahdollisesti vahingoittavat tekijät eli uhat. Uhkien tunnistamisella ja uhka-arvioon liitetyillä riskiarvioilla voidaan määritellä ne osa-alueet, jotka ovat suojattavan omaisuuden kannalta oleellisia.

Syvyyssuuntainen puolustus muodostuu turvavyöhykkeistä, joilla jokaisella on oma merkityksensä ja tehtävänsä uhan havainnoinnissa, estämisessä, rajoittamisessa, viivästyttämisessä sekä torjumisessa. Periaatteena on, että päästäkseen suojattavaan kohteeseen on uhan aiheuttajan läpäistävä kaikkien vyöhykkeiden turvakontrollit. Turvakontrolleja voivat olla esimerkiksi voimassa olevat ohjeet, hallinnolliset järjestelyt, portit, ovet, kulunvalvontapisteet, biometrinen identifiointi, turvakoodit ja saattotoimet.

Teknologia ja teknologian kehittyminen antaa paljon mahdollisuuksia erilaisten turvakontrollien muodostamiseen. Älykkäillä analysointijärjestelmillä voidaan ennalta havaita mahdollisen uhan muodostumista ja käynnistää uhkaan liittyviä vastatoimia. Turvatekniikalla voidaan myös merkittävästi vähentää inhimillisten tekijöiden vaikutusta tärkeiden kohteiden suojaamisessa.

Uhkatilanteissa on kuitenkin merkityksellistä nopea reagointi uhan aiheuttajan toimintaan. Operatiivista henkilöstöä tarvitaan tuottamaan reagointi eli vaste haitalliseen toimintaan.

Erityisesti on huomioitava yrityksen sisältäpäin muodostuvat uhat. Nämä uhat voivat ilmetä millä tahansa yrityksen turvallisuusvyöhykkeellä ja kenen tahansa yrityksessä tai sen sidosryhmissä toimivan tahon toimesta.

2 Syvyyssuuntainen puolustus menetelmänä

Syvyyssuuntainen puolustus on kokonaisvaltainen lähestymistapa omaisuuden suojeluun, jossa yritykselle riskejä aiheuttavan uhan perusteella toteutetaan eri turvallisuuden valvontatasoja sen varmistamiseksi, että suojatun omaisuuden käyttöoikeus rajoitetaan niihin, joilla on luvallinen käyttöoikeus [1]. Käyttöoikeuksien ja kulkuoikeuksien hallinta onkin yksi tärkeimmistä keinoista hallita sisäistä ja ulkoista uhkaa.

Syvyyssuuntaisen puolustuksen periaatteiden mukaisesti turvajärjestelmän on oltava vaikutuksiltaan merkittävä omaisuuden, alueiden tai määriteltyjen turvavyöhykkeen valvonnassa. Turvajärjestelmässä on oltava menettelyt havaita, viivyttää ja antaa vaste uhan aiheuttajan pyrkimyksiin päästä suojattaviin kohteisiin. Jotta menettelyt olisivat tehokkaita, uhan aiheuttajan toiminta on keskeytettävä ja neutralisoitava ennen määritellyn vyöhykkeen rajan ylitystä. On huomioitava, että monissa yrityksissä suojattavien arvojen suojaamiseen tarvitaan useita turvavyöhykkeitä. Yrityksen joillakin henkilöstöryhmillä tulee olla pääsy myös suojattuihin kohteisiin, joka voi jo sinällään muodostaa sisäpiiriuhan (Insider threat).

Turvavyöhykkeiden rajoilla on oltava keino havaita, viivyttää ja vastata uhkaan, jotka koskevat luvatonta pääsyä kaikille turvavyöhykkeille. Uhan aiheuttaman riskin perusteella voidaan edellyttää, että syvyyssuuntaiseen puolustukseen tulee sisällyttää useita uhan havaitsemiseen liittyviä menettelyjä, useita viiveitä aiheuttavia fyysisiä järjestelyjä ja useita vasteen muodostamistoimenpiteitä. Edellä mainitut toimenpiteet tulee suunnitella kunkin turvavyöhykkeen vaatimusten mukaisesti huomioiden ympäröivien ja sisältyvien turvavyöhykkeiden turvamenettelyt ja itse suojattavan arvon suojaustarpeet [1].

Useita turvavyöhykkeitä tarvitaan, koska yhden täydellisen suojaavan vyöhykkeen rakentaminen on vaikeaa, ja sisäkkäisten vyöhykkeiden käyttäminen antaa paremman suojautumismahdollisuuden erilaisia uhkia vastaan. Syvyyssuuntaisen puolustuksen lähestymistavassa on otettava huomioon laajasti uhat,

jotka aiheuttavat riskin kullekin turvavyöhykkeelle, ja sen lisäksi millaisia suojaustoimeniteitä eri vyöhykkeillä tulee muodostaa ja miten eri vyöhykkeiden suojaustoimenpiteet integroidaan yhdeksi turvajärjestelmäksi [1].

Yrityksen toiminnan häiriönsietokyky on tehokas silloin, kun syvyyssuuntaista puolustusta sovelletaan kaikilla yrityksen toimialueilla. Sekä fyysiset että hallinnolliset pääsynhallintatoimet otetaan käyttöön vyöhykkeittäin [1].

Syvyyssuuntainen puolustus tarkoittaa kerroksittain rakentuvaa suojausta, mikä käsittää turvallisuuden hallinnolliset, fyysiset, tekniset ja operatiiviset suojausmekanismit, jotka uhan aiheuttajan on voitettava tai kierrettävä tavoitteidensa saavuttamiseksi [2]. Näiden suojausmekanismien yhteensovittaminen muodostaa tasapainoisen ja hallittavan toimintaympäristön uhkia vastaan.

Syvyyssuuntainen puolustus käsitteenä tarkoittaa

- yrityksen turvallisuuden johtamismenettelyjä
- yrityksen uhkien ja suojaustarpeen tunnistamista
- yrityksen toimintaympäristön suojaamista uhkia vastaan
- reagointikykyä uhkatilanteita vastaan
- toimintaympäristön jatkuvaa kehittämistä muuttuvaa uhkakenttää vastaan
- turvajärjestelmän jatkuvuudenhallintaa koko yrityksen elinkaaren ajan.

Yleinen lähestymistapa syvyyssuuntaiseen puolustukseen koostuu useiden puolustuskerrosten toteuttamisesta, mukaan lukien sekä hallinnolliset näkökohdat (menettelyt, ohjeet, hallinnolliset seuraamukset, kulunvalvontasäännöt, luottamuksellisuussäännöt) että tekniset näkökohdat (useita suojakerroksia, joissa on mekanismit uhkien havaitsemiseen ja viivästyttämiseen), jotka uhan aiheuttajan olisi voitettava tai kierrettävä tavoitteidensa saavuttamiseksi.

Ulkoisen uhan torjumisen lisäksi tulee kaikissa näkökohdissa ottaa huomion Insider-uhan vaikutus. Ennakoivien ja suojaavien toimenpiteiden toteuttaminen In-

sider-uhan torjumiseksi on yleensä paljon vaikeampaa kuin toimenpiteiden toteuttaminen ulkopuolisten uhkien torjumiseksi Insiderin tietämyksen, auktoriteetin ja ominaisuuksien vuoksi. Erityisesti Insider-uhkaa torjuttaessa on huomioitava toimenpiteet työntekijöiden pääsynhallintaan, luottamuksellisen tiedon saantiin sekä henkilöiden auktorisointiin.

Syvyyssuuntaista puolustusta kehitettäessä on huomioitava neljä tärkeää osakokonaisuutta:

- Hallinnollisessa kokonaisuudessa on huomioitava menettelyt, prosessit, ohjeet ja seuraamukset, joilla voidaan pyrkiä määrämuotoiseen toimintaan ja estämään poikkeavaa käyttäytymistä [3].
- Fyysisessä kokonaisuudessa on huomioitava rakennukset, rakennelmat, esteet ja maaston muotoilu, joilla voidaan estää tai hidastaa luvatonta kulkua.
- Teknisessä kokonaisuudessa on huomioitava turvatekniikan käyttö, analyysijärjestelmät, tietoliikenne ja sähkönsyöttö.
- Operatiivisessa kokonaisuudessa on huomioitavaa turvajohtaminen, turvavalvonta ja vasteen muodostaminen uhan torjumiseksi.

Näistä osakokonaisuuksista muodostuu kokonaisvaltainen suojausmekanismi, jonka muodostamisessa tulee huomioida yrityksen toimialan erityispiirteet ja paikalliset olosuhteet. Kaikilla toimialoilla erityisen tärkeiksi uhan torjunnassa nousevat toimet uhan havaitsemiseksi, viivyttämiseksi, uhkaan reagoimiseksi ja uhan vaikutusten lieventämiseksi [4].

2.1 Vyöhykkeistäminen

Yrityksen toimintaan liittyy erilaisia vyöhykkeitä ja vyöhyketasoja. Osa näistä vyöhykkeistä voi olla liiketoiminnan luonteesta johtuvia tuotannollisia alueita, paloturvallisuuteen liittyviä rakenteellisia vyöhykkeitä tai turvallisuuteen sekä tietoturvallisuuteen liittyviä fyysisiä tai loogisia rajamäärittelyjä.

Turvavyöhykkeet ovat fyysisesti erotettu toisistaan, ja jokaisella vyöhykkeellä on omat turvajärjestelymenettelynsä ja merkityksensä. Lähtökohtaisesti turvavyöhykkeeltä toiselle siirryttäessä on määritelty käytänteet, joiden perusteella

siirtyminen joko sallitaan tai estetään. Yhtä lailla vyöhykkeiden sisällä ovat kontrollit, joilla pyritään ohjaamaan vyöhykkeen sisäistä liikennettä tarkoituksenmukaisella tavalla ja estämään mahdollisesti haitallinen tai uhan aiheuttama liikenne.

Syvyyssuuntaisessa puolustuksessa lähtöajatuksena on, että yrityksen suojattavimmat kohteet sijaitsevat syvimmillä turvavyöhykkeillä. Turvallisuuskriittisissä yrityksissä voidaan käyttää esimerkiksi turvavyöhykkeiden 3–5-tasoista syvyyttä, joka mahdollistaa kaikkien kriittisimpien kohteiden sijoittamisen usean kontrollitason suojaamaksi.

Kohteen suojaamisen onnistuminen edellyttää, että poikkeavasta toiminnasta saadaan havainto. Sen perusteella on analysoitavissa, voiko havainnon aiheuttaja muodostaa uhan yritykselle. Vyöhykeperusteisessa ajattelussa havaintoja kerätään sekä vyöhykkeen rajalta että vyöhykkeen sisäpuolelta, ja mikäli mahdollista, myös vyöhykkeen ulkopuolelta. Näiden havaintojen ja tietojen perusteella pyritään analysoimaan, edustaako jokin havainto tai joukko havaintoja mahdollisen uhan toiminnalle.

Jokaisen turvavyöhykkeen suojausmenettelyille asetetuissa vaatimuksissa ja toteutetuissa ratkaisuissa on tarkoituksenmukaista käsitellä alueen sijaintia, pääsynhallintaa, havaitsemista, viivyttämistä ja reagointia koskevia menettelyjä [2]. Menettelyt turvavyöhykkeiden turvajärjestelyissä tulisi poiketa toisistaan ja turvajärjestelyjen pitäisi käytännössä tiukentua siirryttäessä sisemmille turvavyöhykkeille.

2.2 Suunnitteluperusteuhka

Uhkaperusteinen suunnittelu tarvitsee tuekseen suunnittelumenetelmän, jolla osoitetaan turvallisuuteen liittyvät riskikohdat ja jonka perusteella voidaan muodostaa vaatimukset syvyyssuuntaisen puolustuksen toteuttamiselle. Osana yrityksen suojausjärjestelmän tavoitteiden sekä vaatimusten määrittelyä, yrityksen tulisi määritellä yritykseen kohdistuvat uhat uhka-arvioinnin perusteella [2].

Yrityksen turvajärjestelmän tavoitteena on estää tahallisesti tai tahattomasti tehtävää haitallista toimintaa. Tämän tavoitteen saavuttamiseksi turvajärjestelmän suunnittelussa tulisi huomioida uhat, joita vastaan suojaudutaan. Kaikkia uhkia vastaan ei voi kuitenkaan suojautua, ja sen takia yrityksessä on päätettävä, mitä uhkia vastaan suojautumalla haitallisten toimien ja toiminnan riskejä voidaan todennäköisemmin pienentää.

Mikäli yrityksellä ei ole regulaation määrittelemää suunnitteluperusteuhkaa, voi yritys itse laatia sen osoittaakseen yrityksen tahtotilaa suojautumisen tasosta. Turvajärjestelyjen suunnittelua helpottaa, jos mietitään, millaisia uhkia yritykseen voi kohdistua, ja kuvataan olosuhteet, joissa uhat voisivat realisoitua.

Edellä esitetty toimintatapa tarjoaa perustan turvajärjestelmän suunnittelulle ja arviointikriteerit turvajärjestelyjen riittävyyden arvioimiseksi. Toimintatavan etuna on se, että turvajärjestelyjen toteutuksessa ei ali- eikä yliarvioida suojautumisen tasoa uhkia vastaan.

Uhkaperusteisessa toimintatavassa keskeistä on määritellä

- turvajärjestelmän suorituskykytavoitteet ja vaatimukset
- turvajärjestelmän suunnitteluperusteet
- kriteerit turvajärjestelmän arviointia varten. [5.]

2.3 Uhkakuvaukset

Uhkakuvaus on kuvaus uhan aiheuttajan ominaisuuksista, joka voi aiheuttaa haitallista toimintaa, kuten esimerkiksi tietojen varastamista, sabotaasia tai henkilöiden vahingoittamista. Yrityksen tulle laatia kuitenkin omat uhkakuvauksensa perustuen yrityksen liiketoiminnan lähtökohtiin ja yritys tai toimialakohtaisiin uhkiin.

Uhkien arviointi on muodollinen prosessi, jolla kerätään, organisoidaan ja arvioidaan tietoja olemassa olevista tai mahdollisista uhista, jotka voivat johtaa haitalliseen toimintaan. Uhkien arviointiprosessi on keskeinen osa riskinarviointia,

jonka tarkoituksena on tunnistaa järjestelmien haavoittuvuudet ulkoisille ja Insider-uhille. Uhkien arviointiprosessin tuloksena saadaan uskottava arvio ja kuvaus potentiaalisten uhkien aiheuttajien motivaatiosta, aikomuksista ja kyvyistä, joita vastaan suojausjärjestelmät tulee suunnitella ja arvioida. Tällaiset määritelmät mahdollistavat turvallisuusjärjestelmän suunnittelun riskienhallinnan menettelyin. [5]

Uhka-analyysi luodaan tunnistetun uhkatilanteen perusteella ja uhkiin liittyvästä kokemustiedosta. Uhka-analyysin ei ole tarkoitus olla yhdistelmä todellisista vallitsevista uhista, vaan siinä on otettava huomioon myös mahdolliset tulevaisuuden uhat. [5.]

Uhkien arvioinnissa tuli ottaa huomioon

- globaalit ja kotimaiset uhat
- uskottavat uhat, vaikka niitä ei vielä ole todennettu tai niitä ei ole vielä tapahtunut
- yrityksen toiminnassa todennetut tai arvioidut uhat.

Uhkakuvauksen perusteella tulee laatia uhkaskenaariot, joissa kuvataan uhan aiheuttajan tapoja toteuttaa uhkakuvauksen mukainen uhka. Uhkakuvaukset tulisi tehdä suojattaville kohteille muodostuvien seurausten vakavuuden perusteella. Tämä arvio antaa perustan syvyyssuuntaisen puolustuksen ennalta ehkäisevien ja suojaavien toimenpiteiden toteuttamiselle. [4.]

2.4 Uhan aiheuttaja

Uhkien torjunnan luo haasteelliseksi se tosiasia, että uhan aiheuttaja voi olla kuka tahansa yrityksen sisäinen tai ulkoinen tekijä. Kun yrityksessä laaditaan uhkaskenaarioita, on suunnittelussa huomioitava sekä ulkoiset että sisäiset uhat. Sisäiseksi uhaksi tulee määritellä myös yrityksen henkilöstö ja kaikki yrityksessä työskentelevät henkilöt (Insider), jotka voivat aiheuttaa toiminnallaan uhan yrityksen toiminnalle. [4.]

2.4.1 Insider

Toimintaa uhkaavan Insiderin mahdollinen toiminta yrityksen toiminnoissa on otettava huomioon uhkaskenaarioita määriteltäessä, ja määriteltävä potentiaalisen Insiderin ominaisuudet, tavoitteet ja motiivit. Insiderin huomioiminen uhkaskenaarioissa on tärkeää, koska Insiderillä on laajemmat mahdollisuudet aiheuttaa vahinkoa yritykselle kuin ulkopuolisella tekijällä (Outsider). [4.]

Insider määritellään yhdeksi tai useammaksi henkilöksi, jolla on lupa toimia yrityksessä tai käsitellä yritykseen liittyviä arkaluonteisia tietoja. Insider voi yrittää luvatonta omaisuuden poisvientiä tai sabotaasia tai auttaa Outsideriä uhan toteuttamisessa. Insidereita voivat olla esimiehet, vakituiset työntekijät, urakoitsijat ja palveluntarjoajat, tarkastajat ja vierailijat. Insider voi siis olla missä tahansa suhteessa yritykseen. [2.]

Ymmärrys uhan luonteesta edellyttää uhan aiheuttajien tarkan analyysin sisältäen Outsider- ja Insider-uhan aiheuttajat. Insider-uhan ymmärtäminen on haastavaa, koska uhan aiheuttaja voi olla kuka tahansa yrityksessä toimiva, ja uhka voidaan toteuttaa syvyyssuuntaisen puolustuksen eri vyöhykkeillä. Erityisesti Insideria tarkasteltaessa on huomioitava henkilöiden pääsyoikeudet, heidän tietämyksensä yrityksestä, turvajärjestelyjen tuntemus ja valvonnan menettelyjen tuntemus. [4.]

Mikäli Insider on asemassa, jossa hänellä on vahva luottosuhde ja laajat pääsyoikeudet, on hänellä mahdollisuus valita kohteeksi eniten haavoittuva kohde ja valita sopivin ajankohta uhan toteuttamiseen. Insiderilla on myös laajemmat mahdollisuudet tukea Outsideria ulkoapäin tapahtuviin uhkiin luovuttamalla tietoa ja mahdollistamalla Outsiderin toimintaa. Insiderilla on myös mahdollisuus valmistella toimenpiteitä pitkällä aikavälillä ja odottaa sopivaa ajankohtaa uhan toteuttamiseksi. [4.]

Insider voi olla aktiivinen tai passiivinen ja hänen toimensa voivat olla väkivaltaisia tai väkivallattomia. Insiderin motivaatio voi olla esimerkiksi ideologinen, henkilökohtainen, taloudellinen tai psykologinen. Myös muita motivaation aiheita on

syytä tarkastella, kuten esimerkiksi ulkopuolista pakottamista ja uhkailua. Insider voi suunnitella ja toteuttaa uhkaa joko itsenäisesti tai osana suurempaa joukkoa. Insiderin tai ryhmän toiminta voi olla impulsiivista tai valmisteltua ja hyvin harkittua riippuen henkilön tai ryhmän motivaatiosta. [4.]

2.4.2 Passiivinen ja aktiivinen Insider

Analysointia varten Insider-uhat voidaan luokitella sen mukaan, onko Insiderin rooli passiivinen (esimerkiksi vain arkaluontoisten tietojen kerääminen) vai aktiivinen, Jos Insider on aktiivinen, on arvioitava, onko Insider halukas käyttämään voimaa kohdetta tai henkilöä vastaan. Kun otetaan huomioon uhka-arvio tai yrityksen suunnitteluperusteuhka, arviointiin tulee sisältyä Insiderin mahdollisuus toimia toisen Insiderin tai Outsiderin kanssa yhteistyössä [2].

Passiiviset Insiderit eivät ole väkivaltaisia ja rajoittavat osallistumistaan uhan toteuttamiseen antamalla tietoja, tarkkailemalla toimintaa tai osallistumalla uhan toteutussuunnitteluun [4]. Näiden syiden takia passiivisen Insiderin osuus uhan valmistelussa voi jäädä toteamatta, ja Insider voi jatkaa toimintaansa uhan toteuttamisen jälkeenkin.

Aktiiviset Insiderit sen sijaan voivat tietojen toimittamisen lisäksi olla väkivaltaisia tai väkivallattomia. Aktiiviset Insiderit voivat esimerkiksi olla valmiita avaamaan kulkureittejä, antamaan käytännön apua turvajärjestelyjen ja turvaorganisaation toimintakyvyn heikentämisessä tai harhautuksessa [4].

Väkivaltaiset ja aktiiviset Insiderit pyrkivät päämääräänsä riippumatta siitä, onko teon päämäärä saavutettavissa, aiheuttaako se merkittäviä materiaalisia menetyksiä tai hengenvaaraa itselle tai muille. Teot eivät aina ole rationaalisia, vaan ne voivat olla hyvinkin arvaamattomia [4].

2.4.3 Potentiaalinen Insider

Insiderille ei voida määritellä tyypillistä henkilöprofiilia, sijaintia organisaatiossa tai sen toimitusketjussa. Insider voi sijaita missä tahansa organisaation osassa

ja millä tasolla tahansa johtamisorganisaatiota. Jos ja kun Insider on vaikeasti määriteltävissä hänen organisatorisen asemansa tai työtehtäviensä suhteen, on mietittävä, millä tavoin Insider voi päästä tavoittelemaansa päämäärään. [4.]

Insiderillä voi olla käytössään esimerkiksi

- pääsy suojattavalle alueelle, järjestelmiin, laitteisiin tai työkaluihin
- johtoasema tai muu määräämisasema henkilöstöön tai organisaatioon
- tuntemus rakennuksista ja kulkureiteistä
- tuntemus prosesseista ja menettelytavoista
- tuntemus turva- ja turvallisuusjärjestelmistä
- tieto ja kokemus teknisistä järjestelmistä
- voimankäyttö tai taistelukoulutus
- osaaminen aseista ja räjähteistä
- osaaminen biologisista aseista ja kemikaaleista. [4.]

Kun tarkastellaan Insiderin mahdollisia kyvykkyyksiä, voidaan todeta, että Insider voi toteuttaa tekonsa hyvin laaja-alaisesti rakennuksissa, tietojärjestelmissä, huolto- ja kunnossapitotehtävissä ja logistiikkaketjussa [4]. Insider voi siis olla oman organisaation henkilö tai esimerkiksi yrityksen toimittajaverkoston alihankkijayrityksen henkilö.

2.4.4 Motiivit

Insiderin motivaatiot osallistua tai toteuttaa uhka voivat olla moninaisia. Siksi uhka-analyyseissä tulisikin arvioida mahdollisten potentiaalisten Insidereiden motiiveja ja kyvykkyyksiä. Insiderin motiivit voivat olla hyvinkin erilaisia riippuen yrityksestä, sen toimialasta tai toimittajaverkostosta.

Motiivi voi olla esimerkiksi

- ideologinen
- poliittinen
- psykologinen vaikute

- taloudellinen
- kiristys
- lääke- tai huumeriippuvuus
- koska voin -asenne
- kosto
- ulkopuolinen pakottaminen. [4.]

2.4.5 Kyvykkyydet

Uhan aiheuttajan kyvykkyydet määräytyvät uhan aiheuttajan kokoonpanon ja varustuksen mukaisesti. Kyvykkyyttä määriteltäessä on otettava huomioon ryhmän koko, ryhmittyminen, Insiderin mahdollinen osallistuminen sekä uhan aiheuttajan todellinen kyky ja varallisuus. Huomioon on myös otettava uhan aiheuttajan taktiikat, aseet, räjähteet, työkalut, kulkuvälineet, pääsyoikeudet ja taidot. [5.]

Mahdollisen Insiderin kyvykkyydet määritellään tyypillisesti kolmella ominaisuudella:

- Sallittu pääsy: millä laitoksen alueilla sisäpiiriläinen saa tai ei saa kulkea yrityksen eri toimintatilanteissa (esim. normaalit työt, muut kuin työ- tai käyttöajat, huoltoseisokit ja huoltokatkot) tai uhka- tai turvallisuustapahtuman aikana.
- Valtuudet: valtuudet muihin ihmisiin, tiettyihin tehtäviin, tiloihin, järjestelmiin ja laitteisiin.
- Kohdetuntemus: tietämys suojatuista kohteista, laitoksen tai toimitilojen sijoittelusta, turvajärjestelmästä tai miten laitoksesta löytyvät erikoistyökalut ja -laitteet hankitaan ja miten niitä käytetään. [2.]

2.4.6 Suojautuminen

Insiderin aiheuttama uhka on luonteeltaan erilainen kuin Outsiderin aiheuttama uhka, koska Insiderit voivat hyödyntää edellä mainittuja sisäpiirin ominaisuuksia ohittaakseen joitakin teknisiä, hallinnollisia tai fyysisiä suojaustoimenpiteitä luvattoman toimen helpottamiseksi. Insiderit voivat pitkän ajan kuluessa suorittaa tehtäviänsä uhan valmistelemiseksi useiden erillisten toimien avulla. Tämä voi

vähentää heidän havaitsemismahdollisuuttansa ja siten lisätä uhan onnistumisen todennäköisyyttä. Sisäpiiriläisillä voi myös olla enemmän tietoa ja taitoa toteuttaa uhka ja tarvittaessa mahdollisuus valita haavoittuvin kohde ja paras aika suorittaa haitallinen teko. [2.]

Jotta suojattavia kohteita voidaan suojella haitallisilta teoilta, jotka ovat yhdensuuntaisia yrityksen laatimien uhka-arvioiden kanssa, tulee turvajärjestelmän suunnittelussa huomioida menettelyt, joilla tarvepohjaisesti määritellään henkilöiden tai laitteiden pääsy suojattaviin kohteisiin ja minimoidaan Insiderin mahdollisuus tehdä haitallisia tekoja. Esimerkiksi esteiden käyttö yhdessä tehokkaan valvonnan ja vartioinnin kanssa voi estää Outsiderin pääsyn suojattavaan kohteeseen, kun taas suojattavan kohteen eristäminen ja lukitseminen voi aiheuttaa merkittävän viiveen jopa sisäpiiriläisille [2].

2.4.7 Uhan ennaltaehkäisy

Insider-uhan ennaltaehkäisyssä tärkeää on tunnistaa ei-toivottua käyttäytymistä ja ominaisuuksia, jotka voivat ilmentää motivaatiota uhan toteuttamiseksi. Ensimmäinen ja merkittävin vaihe välttää Insiderin toimintaa yrityksessä, on riittävissä määrin tarkistaa henkilöstön ja toimitusketjussa toimivien henkilöiden taustat. Viitteitä potentiaalisen Insiderin havaitsemiseksi ovat esimerkiksi rikosrekisterin tarkastaminen, taloudellisten tietojen selvittäminen, psykologinen testaus ja terveystietojen selvittäminen. Kyseiset toimenpiteet on syytä suorittaa ennen henkilön palkkaamista. Alihankintaketjussa toimittajalta tulisi edellyttää toimintaan osallistuvien osalta vastaavat ennakkotarkastelut ennen tehtävien aloittamista. Esitetyt tarkastukset on tehtävä määräajoin, jotta voidaan varmistua, että henkilöön liittyen ei ole tullut muutoksia heidän riskiprofiiliinsa [4].

Tärkeää on myös rajoittaa henkilöstön pääsyä niille alueille, joilla uhkien toteutumisesta on suurinta haittaa. On tärkeää myös rajoittaa auktoriteettien mahdollisuutta vaikuttaa toimintaan, samoin kuin rajoittaa tietoa kriittisistä kohteista ja niiden suojausmenettelyistä [4].

2.5 Riskien hallinta

Riskiin perustuva lähestymistapa on iteratiivinen prosessi, jossa tunnistetaan ja arvioidaan riskejä: kehitetään, arvioidaan, valitaan sekä toteutetaan toimenpiteitä riskien pienentämiseksi. Lähestymistapaa voidaan käyttää ohjaamaan ennaltaehkäisyä, havaitsemista, reagointia, lieventämistä ja palautumista uhkista aiheutuvien seurausten minimoimiseksi. Lähestymistavalla voidaan tukea päätöksentekoa, kuten strategista suunnittelua; talousarvion laatimista, tutkimuksen ja kehityksen priorisointia ja operatiivisen toiminnan suunnittelua [6].

Riskin arviointiin kuuluu uhkan todennäköisyyden huomioon ottaminen sekä onnistumisen todennäköisyyden ja seurausten tason määrittäminen. Riskin arviointi tukee turvajärjestelmien ja riskien perusteella toteutettavien toimenpiteiden priorisointia [6].

Turvajärjestelmään kohdistuu riski, kun järjestelmällä ei ole riittäviä valmiuksia puuttua uhkaan. Riskianalyysiin kuuluu turvajärjestelmän osa-alueiden, toimenpiteiden tai toimintojen löytäminen, jotka mahdollistavat uhan toteutumisen. Haavoittuvuudet turvajärjestelmässä havaitaan tarkastelemalla uhkia, jotka johtavat suuriin riskeihin. Haavoittuvuutta voidaan pienentää lisäämällä valmiuksia, muuttamalla toimintoja tai menettelyjä [6]. Tunnistettujen turvajärjestelmän riskien perusteella voidaan luoda turvajärjestelmälle vaatimukset, joiden perusteella turvajärjestelmän luotettavuutta voidaan parantaa.

2.6 Vaatimusten hallinta

Riskien pienentämiseksi ja hallitsemiseksi päätetyt korjaavat toimenpiteet tulee kirjata vaatimuksiksi. Vaatimustenhallinnan menettelyin vaatimukset tulee liittää turvajärjestelmän kehittämissuunnitelmaan, ja ne tulee toteuttaa kehittämissuunnitelman mukaisesti.

Turvajärjestelyihin kohdistuvat vaatimukset muodostavat suunnitteluperusteet rakennettaville suojaustoimenpiteille. Vaatimuksilla pyritään kuvaamaan tavoitteet, joiden perusteella voidaan arvioida suojaustoimenpiteiden vaikuttavuutta,

ohjata turvaratkaisujen kehittämistä ja rakentamista sekä arvioida tehtyjen ratkaisujen riittävyyttä uhkakuvien muuttuessa.

2.7 Analyysi

Yrityksen henkilöstö, toimintaprosessit, omaisuus ja tietoaineistot edellyttävät suojautumista uhkia vastaan. Suojautumisessa on otettava huomioon yrityksen ulkopuolelta tulevat uhat ja erityisesti sisältäpäin tulevat uhat. Insiderin torjunta on haastavaa, koska Insiderillä voi olla oikeus suojattavan kohteen hallintaan tai käyttöön. Mitä arvokkaampi suojattava kohde on yritykselle, sitä tarkemmat menettelyt ja fyysiset esteet on luotava suojattavan kohteen turvaamiseksi. On tärkeää tunnistaa, millaisia uhkia yritykseen voi kohdistua, ja niiden perusteella muodostaa suojattaville kohteille riittävät menettelyt vahingollisen teon ennaltaehkäisemiseksi, tunnistamiseksi ja vaikutusten minimoimiseksi. Tunnistetut uhat antavat mahdollisuuden käsitellä yrityksen haavoittuvuuksia riskinhallinnan menettelyin ja kehittää turvajärjestelmää.

3 Turvallisuusjohtaminen

Yritykselle on muodostettava turvallisuuspolitiikka, jossa on todettava organisaation sitoutuminen turvajärjestelyihin. Turvallisuuspolitiikassa on vahvistettava menettelyt yrityksen päätöksenteolle ja henkilöstöön kohdistuville turvakäytänteille. Turvallisuuden kannalta on erityisen tärkeää varmistaa politiikassa se, että henkilöstö ymmärtää, että koko henkilöstön odotetaan noudattavan sovittuja turvallisuus- ja turvakäytäntöjä. Organisaation odotuksiin kuuluvat ammattimainen johtaminen, tietojen suojaaminen, tiedottaminen mahdollisista turvaongelmista ja uhista sekä aktiivisuus turvallisuuteen liittyvien vaaratilanteiden ennaltaehkäisyssä. Nämä yleiset odotukset voidaan vahvistaa dokumentoiduilla turvallisuusperiaatteilla, jotka täydentävät yrityksen turvallisuuspolitiikkaa. [7; 3]

Turvallisuuspolitiikan on sitoutettava ja tehtävä selväksi sen rooli yrityksen toiminnassa. Turvallisuuspolitiikka luo perustan hallintajärjestelmille, jotka ovat oleellinen osa johtamista. Turvallisuuspolitiikan ja -strategian tulee olla selkeä ja viestittävissä koko yrityksen henkilökunnalle sekä yrityksen palvelu- ja alihankintaketjuille. Turvallisuuspolitiikan toimeenpanovastuu on kaikilla yrityksen työntekijöillä oman vastuualueensa mukaisesti [7]. Turvallisuuspolitiikan vaikutus tuleekin näkyä vahvasti yrityksen strategisessa suunnittelussa.

3.1 Johtamisrakenteet

Organisaation kaikkien johtamistasojen on määritettävä organisaation kullekin tasolle sen turvatoimintaan liittyvät roolit, vastuut ja velvollisuudet. Lisäksi organisaation johdon on nimettävä turvallisuudesta vastaava henkilö, jolla on riittävät valtuudet, itsemääräämisoikeus ja resurssit turvatoiminnan jatkuvaan kehittämiseen, toteuttamiseen ja valvontaan. Tämän henkilön on raportoitava organisaation ylimmälle johdolle, jonka vastuut on määriteltävä ja dokumentoitava riittävän yksityiskohtaisesti vastuuepäselvyyksien välttämiseksi [7].

3.2 Johtamisjärjestelmä

Kun tarkastellaan yrityksen kokonaisturvallisuutta, on huomioitava, että turvallisuus on otettava huomioon kaikissa yrityksen toiminnoissa. Sen takia turvallisuuteen liittyvät asiat on huomioitava myös yrityksen johtamisjärjestelmässä. Ilman turvallisuuden integrointia toimintoihin ei saavuteta kokonaistuvallisuutta ja toimintaan voi jäädä haavoittuvia osa-alueita.

Turvallisuuden hallintajärjestelmä on osa yrityksen johtamisjärjestelmää. Yrityksen jokaisen toiminnon on noudatettava hallintajärjestelmää toiminnon turvajärjestelyihin liittyvien odotusten ja prosessien määrittelemiseksi sekä niiden ylläpitämiseksi. Hallintajärjestelmässä tulee olla menettelyt turvatoiminnan edistymisen mittaamiseksi, vaatimustenmukaisuuden arvioimiseksi, suorituskyvyn parantamiseksi kokemusten perusteella sekä menettelyt hallintajärjestelmän muutosten hallitsemiseksi [7].

Turvallisuuden hallintajärjestelmän tulee tukea kokonaisturvallisuuden kehittämistä, ja siihen tulisi sisällyttää ainakin seuraavat asiakokonaisuudet:

- turvallisuuspolitiikka
- turvallisuuden johtamisen tehtävät ja vastuut
- koulutus ja pätevyys
- operatiivinen työnjohto
- henkilöstön luotettavuuden määrittäminen
- operatiivinen toiminta ja vaste
- tietoturva
- laadunvarmistus
- muutoksenhallinta ja jatkuva kehittäminen
- toiminnan suorituskyvyn mittaus
- itsearviointi ja ulkoiset asiantuntija-arvioinnit
- valmiussuunnitelmat ja -harjoitukset (sisältäen jatkuvuussuunnittelun)
- huolto ja kunnossapito
- turvallisuuspalautteet. [7.]

Turvallisuuden johtamisen puutteet, turvallisuuskulttuurin puuttuminen, huono turvallisuustietoisuus ja turvallisuuden kehittämisohjelman puutteet voivat mahdollistaa tai edistää ulkoisen uhan tai Insider-uhan mahdollisuuksia [4].

3.3 Turvasuunnitelma

Yrityksen on laadittava turvasuunnitelma osana toimintasuunnitelmaansa. Turvasuunnitelman olisi perustuttava uhkien arviointiin tai suunnitteluperusteuhkaan. Siihen olisi sisällyttävä aihealueita, jotka koskevat turvajärjestelmän suunnittelua, arviointia, täytäntöönpanoa ja ylläpitoa sekä valmiussuunnitelmia. Yrityksen olisi tarkistettava turvasuunnitelmansa säännöllisesti varmistaakseen, että se pysyy ajan tasalla yrityksen kaikissa toimintatilanteissa ja poikkeavissakin käyttöolosuhteissa. [2.]

3.4 Vastuut ja tehtävät

Turvallisuusjohdon on järjestettävä toimintansa vastaamaan johtamisjärjestelmässä turvasektorille määriteltyjä tehtäviä ja vastuita. Keskeisiä turvallisuusjohdon tehtäviä ovat

- turvallisuustietoisuuden ylläpito ja henkilöstön koulutus
- turvallisuusjärjestelmän kehittäminen
- turvallisuusjärjestelmän arviointi
- valvontatoiminnan kyvykkyyden ylläpito
- vastetoiminnan kyvykkyyden ylläpito
- toiminnan jatkuvuuden hallinta.

3.5 Turvallisuuskulttuuri

Yrityksen turvajärjestelyjen suunnittelu lähtee hyvästä turvallisuuskulttuurista. Yrityksen työntekijät muodostavat toiminnallaan ja asenteillaan yritykselle ominaisen turvallisuuskulttuurin. Turvallisuuskulttuurilla on suuri merkitys siihen, miten yritys onnistuu turvajärjestelmänsä toteuttamisessa. Yleinen ymmärrys, halu

ja tavoitteellisuus luovat edellytykset turvallisuuskulttuurin rakentamiselle, sen ylläpidolle ja kehittämiselle.

Kun luodaan perusteita hyvälle turvallisuuskulttuurille, on yritysjohdon osoitettava motivaationsa turvatoimintojen kehittämiseen, ja johtajuudellaan haettava koko organisaation sitoutumista ja vastuullisuutta turvallisuuden ylläpitämiseen ja sen jatkuvaan kehittämiseen. Vahvan turvakulttuurin kehittämisessä on oltava mukana yrityksen kaikki toiminnot ja yksilöt sekä kaikki yrityksen sidosryhmät, joiden toiminnalla voi olla merkitystä yrityksen turvallisuuteen. Kaikkien näiden toimijoiden on sovellettava toiminnassaan määriteltyä turvapolitiikkaa. Toimijoiden on kehitettävä asianmukaiset hallintorakenteet, osoitettava riittävästi resursseja ja toteutettava asianmukaiset johtamisjärjestelmät turvan kehittämiseksi ja sen ylläpitämiseksi.

Yrityksen turvallisuuden toteuttamiseen osallistuvien organisaatioiden tulisi priorisoida turvallisuuskulttuuri, sen jalkauttaminen ja sen jatkuva kehittäminen. Nämä toimenpiteet ovat välttämättömiä turvallisuuskulttuurin muodostumiselle ja sen vaikuttavuuden varmistamiselle [2].

Yrityksen ja sen sidosryhmien johtajilla on keskeinen rooli turvallisuuskulttuuriin kehittymisessä omien johtamiskäytäntöjensä ja -menettelyjensä kautta. Keskeistä on henkilöstön motivoiminen ja jatkuva turvamenettelyjen parantaminen. Vaikuttavan turvallisuuskulttuurin tuloksena yksilöt omaksuvat holistisen lähestymistavan turvallisuuteen, ja he reagoivat nopeasti ja oikea-aikaisesti mahdollisiin uhkiin [2].

Koko henkilöstön ja erityisesti turvatoimia toteuttavan organisaatioiden tulisi asettaa etusijalle turvallisuuskulttuurin kehittäminen ja sen implementointi kaikkiin yrityksen toimintoihin ja yrityksen toimitusketjuihin. Turvallisuuskulttuurilla on tärkeä rooli sen varmistamisessa, että yksilöt ja organisaatiot pysyvät valppaina ja että uhan ehkäisemiseksi ja torjumiseksi ryhdytään toimenpiteisiin. Hyvä turvallisuuskulttuuri antaa varmuuden siitä, että koko turvajärjestelmä on motivoitunut ja osaava ehkäistäkseen, havaitakseen, viivyttääkseen ja vastatakseen haitallisiin tekoihin yritystä kohtaan. [7.]

Tehokas turvallisuuskulttuuri on riippuvainen sen asianmukaisesta suunnittelusta, henkilöstön koulutuksesta, tietoisuudesta, käytöstä ja ylläpidosta sekä ihmisistä, jotka suunnittelevat, operoivat ja ylläpitävät koko turvajärjestelmää [7].

Inhimillinen tekijä vaikuttaa usein turvallisuuteen liittyviin vaaratilanteisiin sekä toimintoihin liittyviin häiriötilanteisiin. Inhimillisiä virheitä voivat aiheuttaa puutteellinen ohjeistus, piittaamattomuus ohjeista, työergonomia, ohjelmistojen ja laitteiston suunnitteluvirheet, riittämättömät organisatoriset menettelyt ja prosessit. Myös yksilön ymmärrys omasta roolistaan ja vastuistaan, sitoutuminen jatkuvaan parantamiseen voivat aiheuttaa inhimillisiä virheitä. Johdon sitoutuminen ja esimerkki edesauttavat inhimillisten tekijöiden vaikutuksien pienenentämisessä. Tämän vuoksi johtajuus ja johtaminen voivat olla erittäin merkittävässä roolissa turvallisuuskulttuurin luomisessa. [7]

Hyvin johdetulla turvallisuuskulttuurin viestinnällä pyritään varmistamaan, että turvatoimien toteuttaminen saa niiden merkityksen mukaisen huomion. Turvallisuuskulttuuri edellyttää, että yksilöt reagoivat välittömästi vahvistettuihin tai havaittuihin uhkiin ja viestittävät havainnoistaan niille tahoille, joiden tulisi tietää uhasta [7].

Turvallisuuskulttuuri luo siis pohjan yrityksen turvajärjestelmälle. Johdon ja johtamismallin tulee tukea turvallisuuskulttuurin luomista, ylläpitämistä ja jatkuvaa kehittämistä.

3.5.1 Yksilön rooli

Turvallisuuskulttuuri muodostuu koko yrityksen henkilöstön ja yrityksen sidosryhmien yhteisestä sitoutumisesta, jossa luonnollisesti toimintaan osallistuvalla yksilöllä on omat vastuunsa turvallisuuskulttuurin muodostumiseen. Yksilö on vastuussa omasta käyttäytymisestään ja turvallisuuteen liittyvien periaatteiden, määräysten ja ohjeiden noudattamisesta. Yksilö tulee olla koulutettu siten, että hän tunnistaa käyttäytymisensä vaikutukset ja siitä mahdollisesti aiheutuvat seuraukset [7].

Vaikuttavalle turvallisuuskulttuurille ominaista on määriteltyjen sääntöjen, määräysten ja menettelyjen kiistämätön noudattaminen. Yksilöiden on tunnustettava hallinnollisen, fyysisen, teknisen, operatiivisen ja tietoturvallisuuden merkitys osana turvamenettelyjä. Henkilöstön on noudatettava sovittuja menettelyjä ja oltava paljastamatta tietoja, jotka voivat heikentää tai vahingoittaa yrityksen turvajärjestelmää. Turvallisuuskulttuurin kehittyminen riippuu koko organisaation ja työyhteisön yhteistyöstä. Henkilöstön on ymmärrettävä, miten organisaation erilaiset roolit ja toimintojen väliset toimivat rajapinnat edistävät turvallisuuden kehittämistä ja ylläpitämistä [7].

3.5.2 Holistinen lähestymistapa

Vahva uskomus siihen, että yrityksessä voi olla Insider ja että yritystä voi uhata ulkopuolinen uhka ovat perusta turvallisuuskulttuurille. Tämä on erityisen tärkeää, koska tietoisuus mahdollisesta uhasta vaikuttaa ihmisten käyttäytymiseen ja toimintaan, ja siten luo myös pohjan havainnoida toimintaympäristössä tapahtuvia virheitä sekä poikkeamia, ja puuttua niihin [7].

Ilman koko organisaation vahvaa uskomusta ja asennetta mahdollisiin uhkiin, ei todellista turvallisuuskulttuuria ole muodostunut eikä sitä silloin ole olemassa. Turvallisuuden varmistaminen on oltava kaikkien yrityksessä työskentelevien huolenaihe ja vastuu, eikä ainoastaan turvaorganisaation, kuten se yleensä halutaan mieltää [7].

3.6 Tietoturvallisuus

Uhan aiheuttajat, jotka haluavat suunnitella tai toteuttaa yritykseen liittyviä ilkivaltaisia toimia, voivat hyötyä arkaluontoisten tietojen saatavuudesta. Arkaluonteisia tietoja ovat missä tahansa muodossa (ohjelmistot mukaan luettuina) tiedot, joiden luvaton luovuttaminen, muuttaminen, hävittäminen tai käytön epääminen voisi tuottaa haittaa yritykselle. Tällaiset tiedot ovat sen vuoksi yksilöitävä, luokiteltava ja suojattava asianmukaisin toimenpitein [2].

Yrityksen on laadittava sisäiset toimintaperiaatteet ja menettelyt, joilla suojataan yrityksen hallussa olevien tai käsittelemien salassa pidettävien ja arkaluonteisten tietojen luottamuksellisuutta, eheyttä ja saatavuutta yrityksen turvallisuuspolitiikan ja asiaa koskevien kansallisten lakien ja vaatimusten mukaisesti [2].

Myös osa turvajärjestelyihin liittyvistä tiedoista on arkaluontoista tietoa, ja niiden luvaton saanti voisi vaarantaa yrityksen turvajärjestelyt. Yleisten turvallisuusperiaatteiden mukaisesti arkaluonteisten tietojen saatavuus olisi annettava ainoastaan niille, joiden luotettavuus on osoitettu ja joiden on tiedettävä turvajärjestelyistä tehtäviensä hoitamista varten. Turvadokumentaatio voidaan jakaa eri luottamustason dokumentaatioiksi, jotta jokainen osa voidaan tarvittaessa jakaa niiden kanssa, joilla on kyseisestä osa-alueesta tarve tietää ja henkilöillä on asianmukainen todettu luotettavuustaso [2].

3.7 Analyysi

Erittäin suuri merkitys yrityksen omaisuuden suojaamisella on yrityksen johtamismallilla. Jotta yritys toimisi turvallisuustietoisesti, on sen huomioitava turvajärjestelyt yrityksen jokaisella toimintatasolla. Yrityksen johtamisjärjestelmän on tuettava kokonaisturvallisuuden kehittämistä. Erityisen tärkeää on vaikuttavan turvallisuuskulttuurin muodostuminen. Ilman vaikuttavaa turvallisuuskulttuuria henkilöstö ei sisäistä turvallisuuden merkitystä, ja tilanne voi johtaa sääntöjen ja määräysten laiminlyöntiin ja siten voi mahdollistaa uhkatilanteiden muodostumisen. Turvallisuutta ja sen toteutumista tulee johtaa yrityksessä. Turvallisuuden johtamisen tulee olla suunnitelmallista ja tavoitteellista.

4 Turvajärjestelyjen osa-alueet

4.1 Hallinnollinen turvallisuus

Hallinnollinen turvallisuus muodostuu toimenpiteistä, joilla voidaan hallinnollisin keinoin vähentää uhan aiheuttajan mahdollisuutta päästä suojattaviin kohteisiin ja tunnistaa suojattavia kohteita. Myös henkilöstön rekrytointi ja sen kouluttaminen ovat osa hallinnollista turvallisuutta.

Hallinnollisten ennaltaehkäisevien toimenpiteiden tavoitteena on vähentää uhkasta aiheutuvaa riskiä ja minimoida Insiderin todennäköisyyttä uhkaavaan tekoon. Ennaltaehkäisevinä toimenpiteinä suositellaan seuraavia toimenpiteitä:

- Työntekijöiden henkilöllisyyden todentaminen. Varmistetaan, että henkilön on juuri se henkilö, joka väittää olevansa.
- Luotettavuuden arviointi. Luotettavuusarvioinnit ovat jatkuvia arviointeja henkilön rehellisyydestä ja luotettavuudesta sekä työsuhdetta edeltävänä aikana että työsuhteen aikana. Luotettavuusarvioinnin tarkoituksena on tunnistaa henkilöiden motivaatiossa tai käyttäytymisessä tapahtuvia muutoksia. Luotettavuus arviointeihin voidaan liittää myös lääkärin lausunnot henkilön kyvykkyydestä suoriutua tehtävästään sekä arvio henkilön henkisestä tilasta.
- Satunnaisten työntekijöiden ja vierailijoiden saatto ja valvonta työtehtävien aikana. Konsultit, vuokratyöntekijät, kuten huolto-, kunnossapito- tai rakennustyöntekijät tulevat usein hankintaketjun urakointi- tai alihankintayrityksistä, ja heidän luotettavuusarviointinsa voi olla puutteellinen. Vuokratyöntekijöiden ja vierailijoiden luotettavuutta ei kaikilta osin pystytä todentamaan johtuen Suomen lainsäädännöstä.
- Turvallisuuskulttuuri ja turvallisuustietoisuus. Vahvan turvallisuustietoisuusohjelman toteuttaminen henkilöstölle ja koko hankintaketjulle edistää organisaation turvallisuuskulttuuria. Vahva turvallisuustietoisuusohjelma edellyttää selkeää turvallisuuspolitiikkaa, turvakäytäntöjen täytäntöönpanoa ja jatkuvaa koulutusta.
- Tietojen luottamuksellisuus (tietoturva). Turvajärjestelmää tai suojattavia kohteita koskevat tiedot (esim. suojattavien kohteiden sijainti, työmaakartat tai erityiset piirustukset järjestelmistä tai laitteista) suojaaminen auttaa suojaamaan ulkoiselta ja Insider-uhalta.
- Turvajärjestelyjen näkyvyys. Luodaan yrityskuvaa korkean turvatason yrityksenä, ja tuodaan turvallisuuteen liittyvät menettelyt näkyviksi yrityksessä. [4.]

Yrityksen on varmistettava, että turvajärjestelyjen ylläpitämiseksi on määritelty riittävät resurssit koulutukseen ja osaava henkilöstö kehittämiseen, luotettavien ja tarkoituksenmukaisten laitteiden hankintaan, verkko- ja tietoliikenteen varmistamiseen ja toiminnan kehittämisen rahoitukseen [2].

4.1.1 Suojattavat kohteet

Syvyyssuuntaisen puolustuksen järjestämiseksi on tunnistettava ne suojattavat kohteet, jotka ovat kriittisiä yrityksen toiminnan jatkuvuuden kannalta. Luonnollisesti henkilöiden suojaaminen on oleellisinta, mutta on myös luokiteltava erilainen aineellinen ja aineeton omaisuus, jolla on oleellinen merkitys yrityksen toiminnassa.

4.1.2 Suojattavien kohteiden tunnistaminen

Kohteen tunnistaminen määrittää, mitkä yrityksen henkilöryhmät, tieto, prosessit, materiaalit ja laitteet on suojattava uhalta. Kohteiden tunnistamisen neljä vaihetta:

- Ymmärretään kohteiden suojaamisen tavoitteet, eli miksi suojataan.
- Yksilöidään turvallisuuden kannalta tärkeät kohteet, mukaan lukien järjestelmät (tietokonepohjaiset järjestelmät ja tiedot), jotka on suojattava uhkilta.
- Määritellään jokaisen suojattavan kohteen vahingoittumisesta aiheutuvat seuraukset.
- Laaditaan kohdekuvaukset, joihin sisältyvät kuvaukset kustakin suojattavasta kohteesta, sen suojausluokasta ja kohteen sijainnista [2].

Edellä mainitut kuvaukset auttavat ymmärtämään, mitkä ovat seuraukset, jos kyseisiä kohteita ei suojata riittävästi, ja miten kohteiden suojaus voidaan hoitaa kokonaisvaltaisesti.

4.1.3 Testaaminen, harjoittelu ja koulutus

Toiminnan tulee olla riittävästi ohjeistettua. Tämä tarkoittaa normaaliin toimintaan liittyvää ohjeistusta ja erilaisten poikkeustilanteiden ja uhkatilanteiden varalle laadittua ohjeistusta. Uhkatilanteita varten laadittu ohjeistus on lähtökohtaisesti salassa pidettävää ja siihen tulisi olla pääsyoikeus ainoastaan uhkatilanteiden hallintaan liittyvällä henkilöstöllä.

Pelkkä ohjeistus ei sinällään riitä, vaan ohjeistuksen mukaista toimintaa on myös testattava ja harjoiteltava. Testaamista voidaan suorittaa esimerkiksi pöytätestauksena tai kenttätestauksena. Oleellista testaamisessa on yrittää löytää heikkouksia ohjeistuksen mukaisessa toiminnassa ja kehittää kerätyn tiedon perusteella toimintaohjeistusta. Harjoitustoiminta tulee olla säännöllistä ja harjoitustoimintaan tulee ottaa mukaan keskeiset henkilöstöryhmät ja viranomaiset, joilla on merkitys uhan torjunnassa tai uhkatilanteesta palautumisessa.

Syvyyssuuntaisen puolustuksen suorituskyvyn testaaminen tulee aloittaa jo turvajärjestelmän suunnitteluvaiheessa. Tehdyt suunnitelmat tulee testata tarvittavilla analyyseillä, simulaatioilla ja harjoituksilla. Eri sidosryhmien mukaan ottaminen testaamiseen parantaa järjestelmän luotettavuutta ja antaa mahdollisuuden tarkastella järjestelyjä myös turvajärjestelmän soveltuvuudesta yrityksen operatiiviseen toimintaan.

Käytettävissä on useita turvajärjestelmän suorituskykyyn perustuvia lähestymistapoja, jotta voidaan arvioida turvajärjestelmän tehokkuutta. Suorituskykyyn perustuvia arviointimenetelmiä ovat:

Reittianalyysi. Tähän arviointimenetelmään kuuluu aikajanan rakentaminen erilaisille uskottaville uhkaskenaarioille, joita uhan aiheuttaja saattaa käyttää päästäkseen tavoitteeseensa. Aikajanan perusteella analyysillä määritetään, onko olemassa varmuus siitä, että hyökkäys havaitaan sellaisessa vaiheessa, kun vasteaikaa on jäljellä riittävästi, jotta vartiosto voi keskeyttää uhan aiheuttajan toiminnan. Tyypillisesti vasteajat mitataan tai arvioidaan kvantitatiivisesti suorituskykytesteihin perustuen.

Simulaatiot. Tämä arviointimenetelmä sisältää tietokonepohjaiset simulaatiot turvajärjestelmästä tai pöytäharjoitukset, joiden avulla voidaan ottaa huomioon turva- ja valmiussuunnitelmien tehokkuus. Näitä työkaluja käytetään tyypillisesti arvioimaan turvajärjestelmän yleistä suorituskykyä simuloidun uhan aiheuttajan havaitsemiseksi, sen toiminnan keskeyttämiseksi ja neutralisoimiseksi. Simulaatioiden avulla voidaan myös keskittyä tiettyihin näkökohtiin, kuten vasteen tehokkuuteen vastustajan neutralisoimiseksi (eli estää vastustajaa suorittamasta tekoa havaitsemisen ja keskeytyksen jälkeen).

Harjoitukset. Tämä arviointimenetelmää voidaan käyttää turvajärjestelmän tiettyjen osien arviointiin, kuten esimerkiksi hälytykseen reagointiin ja rajoitetusti voimankäyttöharjoituksiin, jotka voivat edustaa yksittäisiä tapahtumia uhkaskenaarioista tai tapahtumaketjuja.

Yhdistelemällä edellä mainittuja arviointimenetelmiä voidaan kompensoida yksittäisen menetelmän puutteita [2].

Simulaatiot ja harjoitukset suoritetaan yleensä osana uhka-analyysiä, jossa erilaiset oletetut hyökkäysskenaariot tunnistetaan ja käytetään harjoitusten perustana sen määrittämiseksi, kuinka tehokkaasti suojausjärjestelmä toimii kussakin skenaariossa. Skenaarioanalyysi perustuu yleensä reittianalyysiin testaamalla erilaisia menettelyjä, joita vastustaja voi käyttää anturien, esteiden ja viestintäjärjestelmien häiritsemiseen tai vastevoiman minimoimiseen.

4.2 Fyysinen ympäristö

Fyysinen suojausjärjestelmä on osa kokonaissuojausta, ja se yhdessä vartioston kanssa muodostaa keskeisen rungon suojattavan kohteen turvaamiseksi. Fyysisen suojauksen järjestelmien on tarkoitus estää haitallisesta toiminnasta aiheutuvat seuraukset. Mitä vakavammat seuraukset ovat, sitä tärkeämpää on luottaa siihen, että fyysinen suojaus on tehdyn uhkaperusteisen suunnittelun perusteella riittävä. [5.]

Fyysisen suojaamisen tavoitteena on muodostaa pelote, edesauttaa uhan havaitsemista, viivästyttää ja muodostaa aikaa vasteen muodostamiselle. Pelote saavutetaan, jos mahdolliset vastustajat pitävät yritystä vahvasti suojattuna kohteena ja päättävät olla toimimasta sitä vastaan, koska he arvioivat onnistumisen todennäköisyyden liian alhaiseksi tai arvioivat mahdollisten kielteisten seurausten olevan itselleen liian suuret. Fyysisen pelotteen edistämiseksi voidaan käyttää esimerkiksi kieltotauluja, yrityksen vartioston näkyvää läsnäoloa, kirkasta valaistusta, ikkunoiden kaltereita ja ajoneuvoesteitä [2].

4.2.1 Fyysiset esteet

Fyysiset esteet tulee asettaa turvajärjestelyvyöhykkeille ja niiden rajoille siten, että uhkan aiheuttajaa viivästytetään merkittävästi, jolloin uhan aiheuttaja menettää omia resurssejaan ohittaakseen fyysiset esteet. Samalla vasteelle muodostuu aikaa keskeyttää uhan aiheuttajan toiminta ennen teon loppuunsaattamista.

Fyysisten esteiden tulee muodostaa tasapainoiset esteet eri uhkaskenaarioille. Fyysiset esteet suunnitellaan perustuen suojattavalle kohteelle asetettuihin suojausvaatimuksiin. Tarkoituksenmukaista on sijoittaa esteet uhan aiheuttajan oletetuille hyökkäysvektoreille. Viivästymisen määrää säädellään käytettyjen esteiden luonteella. Tunnistetuille hyökkäysvektoreille tulisi asettaa useita erityyppisiä fyysisten esteiden tasoja, jotka yhteisvaikutukseltaan estävät uhan aiheuttajan pääsyn suojattuun kohteeseen. Fyysisen suojauksen mitoituksessa on otettava huomioon erilaiset välineet ja taidot, joita uhan aiheuttajalla on oletettu uhkaskenaarioiden perusteella olevan käytössään.

Hälytysten arvioinnin tueksi ja todentamiseksi olisi tarkoituksenmukaista asettaa fyysisten esteiden yhteyteen turvavalvontajärjestelmiä, jotta voidaan selkeämmin havainnoida uhan aiheuttaja ja mahdollisesti sen kyvykkyyttä uhan toteuttamiseen. Tämä järjestely viivästyttää uhan aiheuttajan etenemistä fyysisellä esteellä ja lisää uhan havaitsemisen todennäköisyyttä [2].

4.2.2 Aidat ja ajonestolaitteet

Aidoilla tulisi rajata tärkeitä kohteita kuten tehdasalueita ja merkittäviä kohteita, kuten muuntamoja ja varastorakennuksia. Aidoilla voidaan rajata ja ohjata luvallista kulkua suojattavien kohteiden läheisyydessä ja samalla luoda selkeä valvontalinja luvattoman kulun havaitsemiseksi.

Ajoneuvoporttien ja niiden lähestymissuuntien nopeuksia madaltavilla ratkaisuilla voidaan vähentää todennäköisyyttä, että niitä vasten ajettavat ajoneuvot rikkovat portit. Lähestymistiet, joilla on useita nopeutta hidastavia mutkia portin kummallakin puolella, vähentävät lähellä porttia olevien ajoneuvojen nopeutta ja lisäävät siten ajoneuvoesteiden tehokkuutta. Joka tapauksessa ajoneuvoesteet olisi suunniteltava ja niitä olisi käytettävä siten, että uhkaskenaarioissa kuvatut ajoneuvot voidaan pysäyttää haluttuun pysäytystasoon. Ajoneuvoesteisiin kajoamisen havaitsemiseksi on hyvä käytäntö, että ajoneuvoesteet ja niiden lähiympäristö on teknisillä valvontalaitteilla valvottuja [2].

Ajoneuvoilla voidaan ajaa ja murtautua kevyiden seinärakenteiden, aitalinjojen tai suljettujen porttien läpi. Suojattavalle alueelle tunkeutumisen todennäköisyyden minimoimiseksi ajoneuvon esteet voidaan suunnitella ja asentaa asianmukaisiin ja todennäköisiin paikkoihin rakennuksiin, maalle ja vesialueille [2].

Tiealueelta pääsyä ajoneuvoilla aidan reunustoille tulisi rajoittaa. Aitalinjaa ei ole yleensä mahdollista suojata samalla suojaustasolla kuin aitaan sijoitettuja porttialueita.

4.2.3 Rakennukset ja rakennelmat

Keskeisimmät suojattavat kohteet on sijoitettu rakennuksiin tai rakennelmiin. Rakennuksien mahdollisesti suojaavien aitarakennelmien lisäksi tulee huomioida rakennuksien seinärakenteiden ja mahdollisten kulkuaukkojen rakenteellinen suojaus. Seinärakenteet tulee suunnitella uhkaskenaarioissa määriteltyjen törmäysmitoitusten ja murtomitoitusten mukaisesti.

Rakennusten pintarakenteille, ikkunoille, kulkuaukoille ja sisärakenteille tulee muodostaa suositukset, joita käytetään kaikissa rakennuksissa. Rakennuksille ja sen tiloille tulee myös muodostaa vyöhykkeet, jotka palvelevat sekä rakenteiden lujuuden määrittelyssä sekä rakennusten kulkuoikeusalueiden määrittelyssä.

4.3 Tekniset turvajärjestelmät

Teknisiä turvajärjestelmiä käytetään syvyyssuuntaisessa puolustuksessa havaitsemaan poikkeavia tapahtumia ja seuraamaan sallittua liikennettä. Jokaisella turvajärjestelmällä on oma tehtävänsä turvajärjestelmässä, ja ne yhdessä muodostavat tarkoituksenmukaisen valvontajärjestelmän.

Teknisillä valvontajärjestelmillä on kyky havaita poikkeavia tapahtumia, joka on oleellista riskiarvioinnin ja vasteen muodostamisen kannalta. Valvontajärjestelmät pystyvät tuottamaan tietoa uhkaavista tilanteista, tilanteen muodostajasta ja uhan aiheuttajan liikkeistä.

Jotta turvajärjestelmillä voidaan tukea valvontatoimintaa ja vasteen muodostamista, tulee turvajärjestelmien kyetä kommunikoimaan keskenään ja tuottamaan eri valvontajärjestelmien tuottamaa yhteistä tilannekuvaa.

Tuotetun tilannekuvan perustella perusteella voidaan päätellä mahdollisimman varhaisessa vaiheessa mahdollinen uhkaava toiminta ja ohjata fyysisten esteiden toimintaa tuottamaan lisähidasteita uhan aiheuttajan kulkureitille. Tilannekuvan perusteella pystytään ohjaamaan myös vartioston muodostamaa vastetta oikea-aikaisesti oikeaan paikkaan.

4.3.1 Kulunvalvontajärjestelmät

Kulunvalvontajärjestelmiin kuuluvat laitteet, ihmiset ja menettelyt, joita käytetään kulkuluvan todentamiseen sekä ihmisten, kulkuneuvojen ja materiaalien liikkumiseen. Kulunvalvontajärjestelmiä käytetään hallitsemaan sitä, kenellä on pääsy tiettyyn tilaan tai alueeseen. Kulunvalvontajärjestelmällä ohjataan myös,

milloin henkilöillä on pääsyoikeus tilaan, mistä pääsyoikeus tilaan fyysisesti tapahtuu ja milloin luvallinen kulku voi tapahtua [2].

Kulunvalvontajärjestelmiä käytetään luvitettujen henkilöiden, kulkuneuvojen, materiaalien ja laitteiden sujuvan ja jatkuvan sisäänpääsyn ja poistumisen hallintaan niiden tavanomaisia reittejä pitkin. Vastavuoroisesti kulunvalvontajärjestelmää käytetään estämään, havaitsemaan ja viivästyttämään luvattomien henkilöiden, kulkuneuvojen ja kiellettyjen esineiden liikkumista. Kulunvalvontajärjestelmät antavat vartiostolle tietoja mahdollisesta uhasta tarvittavan reagointivoiman määrittämiseksi ja sen kohdentamiseksi [2; 7].

Yrityksen eri maa-alueelle ja rakennuksiin pääsyn valvomiseksi on asennettava pääsynvalvontajärjestelmä tai pääsynvalvontajärjestelmiä. Koska pääsynhallintajärjestelmät muodostavat sisäkkäisiä suojauskerroksia, se tarjoaa useita havaitsemismahdollisuuksia ja lisää kurinalaista liikkumista sallituilla alueilla. Sisäkkäisten suojausvyöhykkeiden vuoksi sisemmille vyöhykkeille pääsevien kulkuoikeuden saaneiden henkilöiden määrä on pienempi kullakin sisäkkäisellä vyöhykkeellä. Kriittisissä kohteissa tämä rajoitettu pääsynhallinta voi tarkoittaa useita toisistaan riippumattomia kulunvalvontajärjestelmiä. Mitä kriittisemmän suojausalueen kulunvalvonnasta on kysymys, sitä tärkeämpää on suojata sen kulkuoikeuksien myöntämismenettelyt ja kulkuun tarvittavat kulkutunnisteet [2; 7].

4.3.2 Kameravalvontajärjestelmä

Kameravalvontajärjestelmää käytetään rikos- ja tunkeutumisenilmaisujärjestelmän ohella tukemaan yrityksen alue-, tila-, kuori- ja linjavalvontaa.

Keskeisiä valvontakohteita ovat ajoneuvot, ihmiset, turvavyöhykkeiden rajat ja kulkuaukot sekä turvavyöhykkeillä sijaitsevat suojattavat kohteet. Valvonta tulee toteuttaa jatkuvatoimisena, jotta turvallisuuteen liittyvät tapahtumat voidaan tallentaa ja niitä voidaan jälkikäteen käyttää tapahtumien analysointiin ja todisteina tapahtuneesta.

Kameravalvontajärjestelmä on yleensä integroitu kulunvalvontajärjestelmään sekä rikos- ja tunkeutumisenilmaisujärjestelmään. Integraatio mahdollistaa reaaliaikaisen seurannan sekä luvallisiin että luvattomiin kulkutapahtumiin.

Uhkatilanteissa kameravalvontajärjestelmää käytetään tilannekuvan muodostamiseen. Tilannekuva voidaan välittää tarvittaville tahoille videokuvan välityksellä, jolloin päätöksenteko uhkatilanteissa perustuu todelliseen havaintoon.

Turvavyöhykkeiden kameravalvontajärjestelmiä suunniteltaessa tulee ottaa huomioon turvavyöhykkeen valvonnan erityisvaatimukset. Kameravalvontaa suunniteltaessa on otettava huomioon mahdollinen fyysinen erottelu vyöhykekohtaisiin kameravalvontajärjestelmiin. Kameravalvontajärjestelmän videoanalytiikkaa voidaan käyttää esimerkiksi liikkeen havainnointiin, kohteen seurantaan, kasvojen tai rekisterikilpien havainnointiin sekä ääniperusteiseen valvontaan. Analytiikan käyttö helpottaa myös valvomotyöskentelyä, koska analytiikalla voidaan muodostaa automaattiset hälytykset silloin kun asetetut valvontakriteerit täyttyvät.

4.3.3 Tunkeutumisenilmaisujärjestelmä

Tunkeutumisenilmaisujärjestelmää käytetään havaitsemaan mahdolliset tunkeutumisyritykset alueelle tai rakennuksiin. Suojattavien rakennuksien ulko-ovet, ikkunat ja muut kulkemisen mahdollistavat aukot on suojattava tunkeutumisenilmaisujärjestelmän sensoreilla. Tyypillisiä sensoreita ovat liiketunnistimet, kamera-analytiikan liiketunnistus, inertia-, magneetti-, tärinä- tai lasin rikkoutumissensorit. Tunkeutumisenilmaisujärjestelmän sensoreita asetetaan uhka-analyyseihin perustuen oletetuille tunkeutumisreiteille, ulkoalueille, rakennuksiin ja sisätiloihin luvattoman kulkemisen havaitsemiseksi.

Tunkeutumisenilmaisujärjestelmän sensorin antaman hälytyksen perusteella saadaan tietohälytyksen antaneesta kohteesta ja hälytyksen aitous varmistetaan vartioston ja/tai videovalvonnan videomateriaalin perusteella.

4.3.4 Viestintäjärjestelmät

Turvaorganisaation on pidettävä yllä jatkuvaa viestintäkykyä, jolla varmistetaan tehokas tilannehallinta ja tilannetietoisuuden varmistaminen normaali- ja uhkatilanteissa. Mikäli yrityksessä on tiloja tai alueita, joilla viestintä on rajallista, nämä alueet on tunnistettava ja niitä varten on luotava toissijainen viestintämenettely. Kaikilla yrityksen turvallisuuden varmistamiseen liittyvillä henkilöillä tulee olla mahdollisuus liittyä viestintäjärjestelmään ja välittää sekä vastaanottaa turvallisuuteen liittyviä viestintää.

Viestintäjärjestelmiä käytetään Valvomon, vartijoiden ja uhkatilanteissa viranomaisten kanssa tapahtuvan viestinnän hallintaan. Viestintäjärjestelmän tulee olla käytettävissä kaikissa olosuhteissa. Tarvittaessa on voitava muuttaa pääviestintäjärjestelmää ja käyttää toissijaista viestintäjärjestelmää viestinnän varmistamiseksi.

Valvomon ja vartioston välistä kaksisuuntaista viestintää varten on tarjottava turvallinen tiedonsiirtojärjestelmä havaitsemis-, arviointi- ja vastetoimintaa varten. Vartioston ja Valvomon välillä on oltava oma kaksisuuntainen ja turvallinen ääniviestintä. Tehokas viestintä vartioston kanssa antaa tietoa uhan aiheuttajan toimista ja ominaisuuksista sekä mahdollistaa ohjeiden antamisen vartioston sijoittamiseksi [2].

4.3.5 Tietojärjestelmien suojaaminen

Tietojärjestelmien turvajärjestelyjen yleisenä tavoitteena on suojata järjestelmiä hyökkäyksiltä, joilla pyritään keräämään tietoa yrityksestä, sen toimintamalleista ja turvajärjestelyistä. Turvaorganisaation vastuulla on tunnistaa tietojärjestelmät, jotka tarvitsevat suojaa tietoverkkojen kautta tapahtuvia uhkia vastaan [2]. Tietojärjestelmille on laadittava tietoturvakäytännöt ja niiden täytäntöönpanosuunnitelma. Tietojärjestelmät on riittävästi eroteltava toisistaan sekä fyysisesti että loogisesti, jotta vältytään teknisen turvavalvonnan menettämiseltä hyökkäystilanteissa.

4.4 Operatiivinen turvallisuus

4.4.1 Valvomot ja hälytyskeskukset

Tilanteita varten, joissa yrityksen normaali toiminta ei voi vaarantua, tarvitaan turvaorganisaation apua tilanteen normalisoimiseksi. Normaalitilanteessa turvaorganisaatio valvoo määriteltyjen menettelyjen mukaisesti asetettujen turvavaatimusten toteutumista. Suurimmissa ja turvallisuuskriittisimmissä yrityksissä valvontaa johdetaan valvomosta tai hälytyskeskuksesta (Valvomo). Pienemmissä yrityksissä valvonta on usein ulkoistettu turvallisuuspalveluja tarjoaville kumppaneille.

Yrityksellä tulisi olla turvatoimintojensa seurantaan keskittyvä Valvomo tai vastaava toimipiste, jota käytetään hälytysten seurantaan ja arviointiin, vasteen käynnistämiseen sekä yhteydenpitoon vartijoiden, valmiusorganisaation ja yrityksen johdon kanssa. Valvomon tulisi sijaita yrityksen suojatulla alueella, jotta sen toimintoja voidaan jatkaa myös uhkatilanteissa [2].

Valvontajärjestelmät, viestintäjärjestelmät ja monitorointijärjestelmä ovat Valvomon keskeiset työvälineet. Järjestelmät helpottavat tilannekuvan muodostamista, hälytysten seurantaa ja arviointia [2].

Valvomon tehtävänä on valvoa syvyyssuuntaisen puolustuksen periaatteiden mukaisesti eri turvavyöhykkeille asetettujen valvontavaatimusten toteutumista. Poikkeamatilanteissa Valvomo reagoi tapahtuvaan poikkeamaan vasteella. Vasteella tässä yhteydessä tarkoitetaan esimerkiksi reagointia poikkeavaan käytökseen, oven tai anturin vikaantumiseen tai vastetta uhkatilanteeseen.

Koska valvonta perustuu vyöhykekohtaisesti määriteltyihin valvontavaatimuksiin, kyetään vaste ongelmatilanteeseen muodostamaan nopeasti vyöhykkeen ja siellä olevan kohteen asettamien vaatimusten mukaisesti.

4.4.2 Vartiosto

Yrityksellä tulisi olla turvatoimintojensa seurantaan keskittyvä Valvomo tai vastaava toimipiste, jota käytetään hälytysten seurantaan ja arviointiin, vasteen käynnistämiseen sekä yhteydenpitoon vartijoiden, valmiusorganisaation ja yrityksen johdon kanssa. Vaste aloitetaan yleensä viestinnällä uhan aiheuttajalle, että mahdollinen vastustaja on havaittu. Vasteen tehokkuus on riippuvainen siitä, että on saatavilla riittävä määrä asianmukaisesti koulutettuja ja varustettuja turvahenkilöitä tai vartijoita, ja he ovat käytettävissä oikea-aikaisesti oikeassa paikassa. Tavoitteena on saada vaste muodostettua ennen kuin uhan aiheuttaja pystyy toteuttamaan tekonsa. Uhan aiheuttajan neutralisoiminen tai teon keskeyttäminen ovat vartioston keskeinen tehtävä, ja onnistuakseen siinä on vartioston oltava henkilömäärän, välineistön ja koulutuksen osalta paremmin valmistautunut kuin uhan aiheuttaja [2].

Valvomon tehokas tilannekuvan viestintä vartiostolle antaa tietoa uhan aiheuttajan toimista ja ominaisuuksista, kuten esimerkiksi uhan aiheuttajien lukumäärästä, uhkaajien liikkeistä, työkaluista, laitteista, aseista ja ajoneuvoista. Tehokkaalla viestinnällä voidaan myös parantaa vartioston ennakointikykyä ja mahdollisuutta kohdata uhan aiheuttaja vartiostolle edullisessa sijainnissa [2].

Vartioston koulutusohjelma on välttämätön tehokkaan toiminnan kannalta. Kaikkien turvahenkilöiden, Valvomon henkilökunnan ja valmiusjoukkojen on osallistuttava heidän tehtäviinsä ja velvollisuuksiinsa sopivaan koulutukseen [2].

4.4.3 Uhan havaitseminen ja tunnistaminen

Ulkoisten uhkien havaitseminen tapahtuu yleensä jonkun henkilön havainnon tai turvalaiteen antaman hälytyksen perusteella. Haitalliset teot voidaan havaita sensoreilla, henkilöstövalvonnalla ja/tai toimintaprosessien seurannalla. Ulkopuolisen uhan osalta havaitsemistoimenpiteissä keskitytään havaitsemaan uhan aiheuttajan tunkeutuminen turvavyöhykkeille [4].

Uhan tunnistaminen on turvajärjestelmän prosessi, joka alkaa mahdollisesti haitallisella tai muuten luvattomalla teolla tai uhan aiheuttajan havaitsemisella ja hälytyksen antamisella [2]. Uhan tunnistaminen alkaa, kun sensori aktivoituu mistä tahansa syystä. Sensorin aktivoinnilla voi tarkoittaa esimerkiksi laitteisto-anturin laukeamista fyysisessä suojausjärjestelmässä tai henkilön, kuten vartijan, ilmoittamista epäilyttävästä asiasta. [2.]

Havaitsemis- ja arviointijärjestelmillä kohteen tunnistaminen voidaan saavuttaa useiden toisiaan täydentävien rakenteiden ja sensoreiden sekä ihmisten valvonnan yhdistelmällä. Toisiaan täydentäviksi valitaan tietyn turvavyöhykkeen tai esteen sensorit niin, että yritykset ohittaa yksi sensori ovat muiden sensorien havaittavissa ja eri sensorit eivät reagoi samoihin häiriölähteisiin. Satunnaisen tai jatkuvan vartiohenkilöstön nopea lisääminen lisää vastustajan epävarmuutta suojausjärjestelmän tehokkuudesta, mikä vaikeuttaa hyökkäyksen suunnittelua ja suorittamista [2].

Turvajärjestelmän havainnon tehokkuus riippuu sensorijärjestelmien kyvyistä, hälytyssignaalin aktivoinnista, hälytysraportoinnista ja -arvioinnista sekä Valvomon henkilökunnan suorituskyvystä ja mahdollisista vartijoista tai pelastushenkilöstön jäsenistä, joilla on rooli havaitsemisessa. Teknologialla voidaan tehostaa havaitsemisprosessin kaikkia vaiheita. Jos teknologiaa käytetään, havaitsemisjärjestelmässä olisi käytettävä sensoreita ja videojärjestelmiä, jotta saadaan luotettavaa tietoa kohteen tunnistamiseksi ja arvioimiseksi [2].

4.4.4 Viivästäminen

Viivästäminen on fyysisten turvajärjestelmien tehtävä, jolla pyritään hidastamaan uhan etenemistä kohti tavoitettaan, mikä antaa enemmän aikaa tehokkaalle vasteelle. Viivästämistä voidaan toteuttaa osittain myös vartioston toimesta.

Viiveen uhan aiheuttajalle tuottavat ja muodostavat henkilöstö, turvamenettelyt tai fyysiset esteet, jotka toiminnallaan lisäävät uhan aiheuttajan uhan toteuttamiseen kuluvaa aikaa. Useimmat esteet on suunniteltu viivästyttämään Outsiderin

turvavyöhykkeille tunkeutumista sen sijaan, että esteet viivästyttäisivät yrityksen sisältä tapahtuvia ilkivaltaisia tekoja, ja sen vuoksi fyysisten esteiden vaikutus Insideriin on rajallinen. [4.]

Viivästys voidaan saavuttaa yksinkertaisesti pitkillä etäisyyksillä ja vaikeakulkuisilla alueilla, jotka on ylitettävä kohteeseen pääsemiseksi. Näiden lisäksi uhkaa voidaan viivästyttää esteillä, kuten aidoilla, porteilla, ovilla, lukoilla, häkeillä ja aktivoiduilla viivejärjestelmillä. Esteet voivat estää tai kukistaa uhan aiheuttajat, jos he eivät pysty läpäisemään estettä. Jokainen estetyyppi vie aikaa, ennen kuin uhan aiheuttaja tunkeutuu kohteeseensa. Nämä viiveajat ovat tekijöitä, jotka on otettava huomioon suunniteltaessa fyysistä suojausjärjestelmää. Vartijat tai valmiusjoukot voivat viivästyttää edelleen, mikäli ne on sijoitettu tarkoituksenmukaisesti, aseistettu, ja ovat suojattuja uhan välittömiltä vaikutuksilta. [2]

Turvajärjestelmien viivästyselementtien tehokkuuden ensisijainen mittari on aika, jonka vastustaja tarvitsee havaitsemisen jälkeen viivästystä tuottavien toimenpiteiden ohittamiseksi. Viivästyksellä, jonka vastustaja kohtaa ennen havaitsemista, ei ole mitään arvoa suojausjärjestelmän tehokkuudelle, koska tällainen viivästys ei anna lisäaikaa muodostaa vastetta. Viivästyminen on erityisen tärkeä tehtävä tapauksissa, joissa vartiostoa ei ole lähtökohtaisesti sijoitettu lähelle suojattavia kohteita [2].

4.4.5 Vaste

Vaste on sen turvajärjestelmän tehtävä, joka pyrkii keskeyttämään ja neutralisoimaan uhan aiheuttajan ennen haitallisen teon toteutumista. Tyypillisesti tämä tehtävä on määritelty vartiostolle. Vartioston on saatava tieto uhan havaitsemisesta ja riittävät toimintaohjeet uhan aiheuttajan tunnistamiseksi. Vaste pyritään suuntaamaan paikkaan, joka sijaitsee uhkan aiheuttajan ja sen tavoitteleman kohteen välissä ja muodostaa vartiostolle mahdollisimman edullisen tilanteen kohdata uhan aiheuttaja. Vasteen muodostamisen kannalta on oleellista, että uhkahavainnon ja vartioston reagoinnin välinen aika jää mahdollisimman lyhyeksi.

Uhan aiheuttajalle tavoitteen saavuttamiseen tarvittava aika on tunkeutujan tehtäväaika. Esteiden ensisijainen tehtävä on lisätä tunkeutujan tehtäväaikaa ottamalla käyttöön esteitä vastustajan valitsemalla reitillä. Vastustajan on läpäistävä tai ohitettava useita erillisiä esteitä, ennen kuin se pääsee haluttuun kohteeseen. Näiden esteiden läpimenon tai ohittamisen ei välttämättä tarvitse olla yhtä suuri aika, mutta esteet olisi valittava niin, että jokainen edellyttää uhan aiheuttajalta erillistä ja erilaista toimea uhan aiheuttajan liikkuessa kohti kohdettaan.

Havaitsemisen todennäköisyys koostuu todennäköisyyksistä, että uhkaava toiminta havaitaan, että hälytys syntyy ja se raportoidaan ja että hälytys arvioidaan oikein. Mitä lyhyempi havaitsemisaika on, sitä todennäköisempää on, että hälytyksen syy voidaan arvioida ja vartiosto kyetään lähettämään ajoissa keskeyttämään uhan aiheuttajan toimet [2]. Mahdollisen uhan aiheuttajan toiminta katsotaan havaituksi vasta, kun on tiedossa, mikä aiheutti hälytyksen, mikä tietty toiminta aiheutti hälytyksen, missä toiminta tapahtui ja kuinka monta henkilöä tapahtumaan osallistui.

4.5 Analyysi

Hallinnolliset prosessit ja menettelyt antavat hyvän pohjan turvallisuuskulttuurin luomiseen. Henkilöstön, alihankkijoiden ja yrityksen verkostossa toimivien sitouttaminen yrityksen toimintamalliin ja hallinnollisiin menettelyihin ja ohjeistukseen on merkityksellistä turvajärjestelyjen toimivuudelle. Pelkät hallinnolliset toimet eivät riitä, vaan on otettava huomioon myös yrityksen fyysiseen toimintaympäristöön liittyvät tekijät. Tällaisia tekijöitä ovat erimerkiksi rakennukset ja rakennelmat, joissa suojattavat kohteet sijaitsevat, ja mekanismit, joilla tätä infrastruktuuria suojataan. Fyysistä suojaamista ja uhan havainnointikykyä tulee parantaa teknisillä valvontajärjestelmillä. Valvontajärjestelmillä voidaan tehokkaasti rajoittaa henkilöiden liikkumista yrityksen alueella ja varsinkin suojattavien kohteiden läheisyydessä. Uhan toteutumiseen on varauduttava reagointikyvyllä, joka tarkoittaa käytännössä henkilöresurssein tuotettavaa vastetta. Vaste on kyettävä muodostamaan ennen kuin uhan aiheuttaja pääsee tavoitteeseensa. Vastetta voidaan tehostaa fyysisen ympäristön esteillä ja valvontajärjestelmillä toteutetta-

villa sulkutoimilla. Koska uhan aiheuttaja voi olla taho, jolla on mahdollisuus oikeuksiensa perusteella päästä suojattavaan kohteeseen, on erityisen tärkeää pystyä havainnoimaan sekä henkilöstön toiminnan poikkeavuuksia että analysoimaan valvontajärjestelmien dataa.

5 Tutkielman soveltaminen käytäntöön

Tässä luvussa annetaan esimerkki tämän tutkielman soveltamisesta käytäntöön. Esimerkkinä käytetään kuvitteellista yritystä, jonka tarkoituksena on kehittää omaa turvajärjestelmäänsä tilanteessa, jossa yritys on laajentamassa omaa tuotantolaitostaan. Tuotantolaitoksen laajentumisen myötä, yritykselle muodostuu uutta liiketoimintaa, jolla on merkitystä kansalliselle huoltovarmuudelle. Tämän johdosta yritykselle muodostuu lainsäädännöllisiä velvoitteita liittyen turvajärjestelyihin ja niiden kehittämiseen.

5.1 Lähtötilanne

Yrityksellä on toimitilat lähellä suurta asutuskeskusta vilkkaasti liikennöidyllä alueella. Yrityksen omistama maa-alue on osittain rakennettu. Siellä sijaitsee yrityksen pääkonttori ja tuotantolaitos. Maa-alueelle on tarkoitus rakentaa uusi tuotantolaitos, jonka jälkeen koko maa-alue käytetty rakentamiseen. Tuotantolaitoksen rakentamisen yhteydessä yrityksen henkilömäärä kasvaa 300 henkilöstä 600 henkilöön.

Uudessa tuotantolaitoksessa tuotetaan tuotteita, joiden suunnittelutiedot, valmistusprosessi, raaka-aineet ja lopputuotteet ovat suojattavaa omaisuutta. Kyseinen omaisuus säilytetään laitoksen alueella koko tuotantoprosessin ajan.

5.2 Suunnittelu

Yrityksen hallitus on päättänyt aloittaa kehitysprojektin turvajärjestelyjen kehittämiseksi vastaamaan viranomaisten ja liiketoiminnan turvajärjestelyihin kohdistuviin vaatimuksiin. Johtoryhmä edellyttää, että suunnittelussa on otettava huomioon asetetut vaatimukset, henkilöstön määrän kasvu ja taloudelliset reunaehdot. Projektiryhmän tueksi palkattiin turvallisuusalan konsulttiyritys tukemaan nykytilan arviointia ja kehittämissuunnitelman laadintaa.

Projektiryhmä laati kehittämisehdotuksen, jossa se kuvasi keskeiset asiakokonaisuudet, jotka on otettava huomioon yrityksen turvajärjestelmää kehitettäessä. Projektiryhmä päätyi esittämään seuraavaa toimenpidekokonaisuutta turvajärjestelmän kehittämiseksi:

- yrityksen turvallisuuspolitiikan tarkastaminen
- turvallisuuskulttuuriohjelman perustaminen
- koulutussuunnitelman laadinta
- uhkatilanteen kartoittaminen
- Insider uhan arvioiminen
- riskienhallinnan käynnistäminen
- turvallisuusorganisaation kehittäminen
- rakentamissuunnittelun tukeminen
- fyysisten turvajärjestelyjen kehittäminen
- tietotekniikan ja turvajärjestelmien kehittäminen
- operatiivisen turvavalvonnan kehittäminen
- pitkän aikavälin projekti- ja rahoitussuunnitelman laadinta.

5.2.1 Yrityksen turvallisuuspolitiikan tarkastaminen

Yrityksen johtoryhmä, joka koostui yrityksen toimitusjohtajasta ja eri osastojen johtajista, arvioivat yrityksen turvallisuuspolitiikan ajanmukaisuuden ja turvajärjestelyperiaatteet liittyen laadittuun kehittämisehdotukseen. Turvallisuuspolitiikkaan tehtiin tarkennuksia ja niiden perusteella kirjoitettiin yritykselle täydentäviä turvallisuusperiaatteita. Turvallisuuspolitiikan ja turvallisuusperiaatteiden tarkastelun yhteydessä havaittiin useita puutteita yrityksen johtamisjärjestelmässä ja tehtävävastuujaossa. Johtoryhmä tarkensi turvallisuusosaston toiminnallisia vastuita ja nosti turvallisuuden yhdeksi johtoryhmässä seurattavaksi asiakokonaisuudeksi. Samassa yhteydessä perustettiin myös yritykseen turvallisuusjohtajan tehtävä.

Turvallisuusjohtajalle määrättiin tehtäväksi koordinoida turvallisuustoimintaa yrityksessä ja osallistuttaa yrityksen eri osastot turvallisuuden kehittämiseen. Turvallisuusjohtamista varten perustettiin ohjausryhmä, jonka tarkoituksena on kehittää yrityksen kokonaisturvallisuutta.

5.2.2 Turvallisuuskulttuuriohjelman perustaminen

Yrityksessä ei aiemmin ollut kiinnitetty erityistä huomioita turvallisuuskulttuuriin. Yrityksessä oli sen toimintahistorian aikana muodostunut avoin toimintakulttuuri, jossa työntekijöillä oli pääsy yrityksen kaikkiin tiloihin ja tietoon. Turvallisuuskulttuuri ohjelman laadinnan perusteella turvallisuuden ohjausryhmä päätyi seuraaviin toimenpiteisiin:

- Henkilöstöä on koulutettava turvalliseen toimintaan.
- Pääsyä tietoihin ja tiloihin on rajoitettava tarvekohtaisesti.
- Toimintaohjeistuksesta poikkeavaan toimintaan on puututtava.
- Turvallisuustilanteita on harjoiteltava.

Turvallisuuskulttuuriohjelman jalkautusta varten henkilöstölle pidettiin tietoiskuja ja yrityksen intranetiin perustettiin turvallisuussivusto, josta pystyi yhdestä paikasta tutustumaan turvallisuuspolitiikkaan, turvallisuusperiaatteisiin, turvallisuuskulttuurin koulutusmateriaaliin ja keskeisiin turvallisuuteen liittyvään ohjeistukseen. Henkilöstöltä edellytettiin myös koulutusohjelmaan liittyen tentin suorittamista, jossa kerrattiin keskeiset asiat turvallisuuskulttuurista ja turvallisuuskäytänteistä.

5.2.3 Koulutussuunnitelman laadinta

Turvallisuuskulttuurin kehittämisen seurauksena päätettiin koulutus- ja harjoitustoiminnan käynnistämisestä. Suunnitelman tarkoituksena oli kouluttaa henkilöstöä turvallisuuden eri osa-alueilta. Koulutuksessa painotetaan tietoturvallisuutta, kriittisen tiedon käsittelyä, turvallisuustilanteissa toimimista, turvallisuustilanteista raportointi ja turvallisuustilanteista toipumista.

koko henkilöstölle päätettiin järjestää koulutusta turvallisuusperiaatteista, niiden noudattamisesta ja turvallisuuteen liittyvästä lainsäädännöstä, määräyksistä ja ohjeista. Vastuualue- ja toimintokohtaisesti rakennettiin koulutusohjelmat, joiden perusteella henkilöt pystyvät toiminaan eri turvallisuustilanteissa ja huomioimaan henkilöturvallisuuden, omaisuuden suojaamisen ja toiminnan jatkuvuuden.

Koulutusten lisäksi päätettiin järjestää erilaisiin uhkatilanteisiin liittyviä harjoituksia, joissa harjoitellaan erityisesti suojautumista uhkatilanteissa ja tiedottamista uhkatilanteiden aikana.

Uuden tuotantolaitoksen rakentamisen johdosta päätettiin myös lisätä tietoisuutta uudesta liiketoiminnasta sen tuomista muutoksista ja rajoituksista nykyiseen toimintaan. Tämän lisäksi myös uuteen tuotantolaitokseen rekrytoitaville henkilöille päätettiin teettää turvallisuus selvitykset ja aloittaa turvallisuuden koulutusohjelma.

5.2.4 Uhkatilanteiden kartoittaminen

Yrityksessä ei ollut aiemmin arvioitu yrityksen haavoittuvuuksia uhkienhallinnan menettelyin. Uhkien kartoittamista varten muodostettiin eri osastojen asiantuntijoista työryhmä, jonka tarkoituksena oli perehtyä uhkien hallintaan ja luoda yritykselle uhkienhallintamalli. Työryhmä kartoitti julkisista lähteistä saatavaa uhkatietoa ja kävivät sisäistä keskustelua yritykseen kohdistuneista uhkista ja mahdollisista tulevaisuuden uhkista. Uhkien kartoittamisen perusteella laadittiin uhkaskenaariot, joissa tarkasteltiin uhkia tietoturvallisuuden, fyysisen tunkeutumisen, sabotaasiin ja ilkivallan näkökulmasta. Uhkien kartoittaminen yhteydessä havaittiin merkittävä määrä haavoittuvuuksia ja riskejä yrityksen toiminnassa. Työn perusteella päätettiin, että riskien hallintaa tulee tehdä erillisenä toimintona, ja riskien perusteella pitää laatia muutosehdotukset olemassa olevien käytäntöjen ja menettelyjen tarkentamiseksi tai muuttamiseksi. Uhkien ja riskien hallinnasta päätettiin muodostaa jatkuva toiminto ja dokumentoida niihin liittyvät prosessit ja toimintatavat. Uhkakuvausten ajantasaisuus päätettiin arvioida määrävälein ja tunnistaa mahdolliset toimintaan vaikuttavat uudet uhat.

5.2.5 Insider uhan arviointi

Uhka-arviointien yhteydessä huomattiin, että merkittävä määrä yrityksessä toteutuneista uhkatilanteista johtui tai voisi johtua oman henkilöstön toiminnasta tai ohjeistuksesta. Uhka-arvioista ilmeni, että henkilöillä oli mahdollisuus päästä tiloihin, joiden käyttöön heillä ei ollut tarvetta. Varastoanalyyseissä huomattiin, että materiaalihävikit ovat suurempi kuin normaalitilanteissa voisi olettaa.

Uhka-arvioiden perusteella todettiin Insider-uhan torjuminen erittäin vaikeaksi, ja uhan torjumiseksi tunnistettiin seuraavia tekijöitä:

- turvallisuuskulttuurin kasvattaminen
- rekrytoitavien arviointi ja henkilön taustojen tarkastaminen
- uuden henkilön perehdyttäminen turvallisuuskulttuuriin
- uhka- ja häiriötilanteista ilmoittaminen
- henkilöiden työtehtävien ja vastuualueiden määrittely
- pääsynhallinta tietoihin ja tiloihin
- nopea reagointi poikkeamiin
- koulutus ja harjoittelu.

Analyysien perusteella päätettiin määritellä yritykseen turvavyöhykkeet ja yrityksessä määriteltiin tarkemmin jokaisen henkilön työnkuva ja rooli/roolit yrityksen toiminnassa. Henkilön roolien mukaisesti hänelle määriteltiin tarvittavat pääsy- ja kulkuoikeudet tarvittaville turvavyöhykkeille. Samalla päätettiin myös, että kulunvalvontaa tulee suorittaa valvontajärjestelmillä yrityksen alueella.

5.2.6 Riskienhallinnan käynnistäminen

Uhka-analyysien perusteella havaittiin, että yrityksen olemassa olevat riskinhallintamenettelyt eivät ole riittävät, jotta yrityksen kokonaisturvallisuuden hallinta olisi hallittavalla tasolla. Riskienhallintaan perustettiin työryhmä, jonka tarkoituksena on analysoida uhkakartoituksen perusteella tunnistettujen uhkien käsittelyssä havaitut haavoittuvuudet ja riskit. Ryhmän tehtävänä on muodostaa vaati-

mukset ja toimenpidesuunnitelma, miten havaittu riski voidaan estää tai sen vaikutus voidaan minimoida. Toimenpidesuunnitelmassa huomioitiin muutokset nykytoimintaan, nykytoiminnan kehittämistarpeet, rakentamisen aikaiset erityistarpeet ja uuden tuotantolaitoksen käyttöönoton ja tuotantokäytön tarpeet.

Toimenpidesuunnitelmaan perustuen ryhmä laati muutosehdotukset, joilla toimintaa tulisi kehittää. Muutosehdotukset liitettiin osaksi toiminnan kehittämissuunnitelmaa ja asetettiin toteutettaviksi tehtävien priorisoinnin mukaisesti.

5.2.7 Turvaorganisaation kehittäminen

Uhkakartoituksen ja riskienhallinnan perusteella havaittiin, että poikkeaviin ja uhkatilanteisiin reagointi oli liian hidasta. Uhkakartoituksessa havaittiin myös, että yrityksen toimipisteen tekninen valvonta oli puutteellista ja käytettävä teknologia osittain vanhentunutta.

Koska yrityksen liiketoimintaa oltiin laajentamassa ja siihen jatkossa sisältyy turvallisuuskriittisiä toimintoja, oli yrityksen toimipisteen rakennusten ja ulkoalueiden valvontaa tehostettava. Yrityksessä päätettiin, että etänä tehtävän turvallisuusvalvonnan sijasta yrityksen toimipisteeseen tulee luoda oma valvomotoiminto. Valvomo päätettiin sijoittaa uuden rakennettavan tuotantolaitoksen yhteyteen mahdollisimman lähelle kriittisiä kohteita. Samassa yhteydessä päätettiin, että vartioston läsnäoloa pitää lisätä yrityksen alueella kaikkina vuorokauden aikoina, jotta reagointi ja vasteaikaa voidaan lyhentää uhka- ja poikkeustilanteissa. Vasteen muodostamiselle koko yrityksen alueella asetettiin tavoiteaika.

Jotta päätöksenteko eri uhkatilanteissa saataisiin nopeammaksi ja perustellummaksi päätettiin muodostaa tilannekuvajärjestelmä, johon kerätään eri valvontajärjestelmistä ja havainnon tekijöiltä tietoa tilanteen analysoimiseksi. Samalla tilannekuvajärjestelmän tulisi toimia raportoinnin ja jälkikäteen tehtävän tilanneanalyysin työvälineenä. Turvaorganisaation kommunikointivälineitä päätettiin kehittää ja samalla parantaa kommunikointitapoja pelastusviranomaisten ja poliisin kanssa.

5.2.8 Rakentamissuunnittelun tukeminen

Koska muutoksen lähtökohtana oli uuden tuotantolaitoksen rakentaminen, turvaorganisaatio osallistui uuden tuotantolaitoksen suunnitteluun. Turvaorganisaatio oli mukana suunnittelemassa maankäyttöä, uuden tuotantolaitoksen sijaintia, sinne johtavia tiejärjestelyjä ja itse laitoksen rakennetta. Turvaorganisaatio laati erillisen turvasuunnitelman koko laitoksen turvallisuuden varmistamiseksi, jossa otettiin huomioon sekä olemassa oleva liiketoiminta että rakennettava uusi tuotantolaitos. Suunnittelussa otettiin huomioon sekä uuden tuotantolaitoksen rakentamisaikaiset turvajärjestelyt että käytönaikaiset turvajärjestelyt.

Fyysisten turvajärjestelyjen suunnittelussa päätettiin, että koko yrityksen alueella on rajoitettava kulkemista, ja sen johdosta koko yrityksen alue aidattiin ja asetettiin riittävät tekniset valvontalaiteet alueen valvontaan. Alueelle ei päästetty enää kulkuluvattomia henkilöitä. Vieraat ja tavarakuljetukset saatettiin ulkoportilta kohteisiinsa. Alueen valvontaa ja sen näkyvyyttä tehostettiin kiertävällä vartioston valvonnalla. Uusi tuotantolaitos rajattiin aidalla omaksi turvavyöhykkeekseen, jotta voitiin seurata työmaalla työskenteleviä ja sinne suuntautuvaa liikennettä. Uuden tuotantolaitoksen työmaan kulkureitit eristettiin muusta yrityksen toimintaan liittyvistä kulkureiteistä ja logistiikasta.

Rakentamisaikana järjestettiin koulutuksia ja harjoituksia työmaan henkilöstölle turvallisuuskäytännöistä ja turvallisuuskulttuurista. Harjoituksissa perehdyttiin erilaiset uhkatilanteiden ennaltaehkäisyyn, niiden ilmoittamiseen, haittavaikutusten minimointiin ja uhkatilanteista palautumiseen.

Turvaorganisaation vastuulla oli suunnitella koko alueen turvajärjestelyt huomioiden rakentaminen, siirtyminen tuotannolliseen toimintaan ja turvajärjestelyjen jatkuvuuden hallintaan.

5.2.9 Fyysisten turvajärjestelyjen kehittäminen

Turvaorganisaatio vastasi fyysisen ympäristön turvasuunnittelusta. Turvajärjestelyjä varten luotiin ulkoalueille kolme eri vyöhyketasoa. Ensimmäinen vyöhyketaso muodostui koko yrityksen aluetta kiertävästä aidasta. Aidan yhteyteen rakennettiin kameravalvontajärjestelmä ja tunkeutumisenilmaisujärjestelmä. Aidan kulkuaukkoihin muodostettiin kulkuyhteydet, joissa edellytettiin henkilön ja ajoneuvon tunnistautumista. Luvittamattomien ajoneuvojen paikoitusalueet sijoitettiin aidatun alueen ulkopuolelle. Ajotiet yrityksen aidatulle alueelle suojattiin ajonestolaitteilla. Aidatun alueen sisäpuolella rajattiin toimistoalue, varastoalue ja tuotantolaitos omiksi valvonta-alueikseen. Näihin myönnettiin kulkulupa vain tarveperusteisesti.

Rakennuksia varten laadittiin tilaluokitteluohjeet, jotka perustivat tiloissa sijaitseviin kriittisiin toimintoihin, tilassa sijaitsevaan suojattavaan prosessiin tai materiaaliin tai tilassa sijaitsevaan suojattavaan tietoon. Rakennuksen tilat luokiteltiin kolmeen tasoon, joista syvimmällä tilaluokittelutasolla sijaitsivat kriittisimmät kohteet. Vastaavasti kuten ulkoalueilla myös rakennuksissa rajoitettiin henkilöiden kulkuoikeuksia tarve- ja roolipohjaisesti.

5.2.10 Tietotekniikan ja turvajärjestelmien kehittäminen

Yrityksessä ei ollut aiemmin panostettu tekniseen valvontaa, vaan oli luotettu siihen, että yrityksen rakennusten lukitseminen työajan ulkopuolella on riittävä suojautumiskeino uhille. Toimintasuunnitelman mukaisesti turvavalvontajärjestelmiä kehitetään siten, että niiden perusteella voidaan tunnistaa kaikki henkilö- ja ajoneuvoliikenne yrityksen ulkoaidalla ja liikennettä voidaan seurata yrityksen alueella. Yrityksen aitavalvontaa kytkeytyvän tunkeutumisenilmaisujärjestelmän lisäksi rakennettiin ukkoalueelle kattava kameravalvontajärjestelmä. Samalla ulkoalueiden valaisusta parannettiin helpottamaan liikenteen tunnistamista ja vartioston toimintaa huonoissa valaistusolosuhteissa.

Rakennuksien kuorivalvontaa laajennettiin siten, että rakennuksien kaikki kulkuaukot, mukaan lukien kattorakenteet saatettiin turvavalvonnan piiriin. Rakennuksien sisällä eri kulunvalvonta-alueiden välillä edellytettiin kulkutunnisteen käyttöä ja kriittisimmissä kohteissa kulkutunnisteen lisäksi PIN-koodia. Kriittisten kohteiden luvitukset päätettiin toteuttaa kaksivaiheisena, jossa tilan tai tiedon omistajan lisäksi edellytetään turvaorganisaation hyväksyntä henkilön luvittamiselle.

Turvajärjestelmien hälytystiedot kerättiin keskitetysti valvomoon, joka hälytykseen liittyvän riskiarvion perusteella käynnistää ohjaus, opastus tai vastatoimet hälytyksiin liittyen.

5.2.11 Operatiivisen turvavalvonnan kehittäminen

Uhka-arvioinneissa todettiin, että vartiointiliikkeen tekemät määräaikaiskierrokset ja vartiointiliikkeen reagointiaika eivät ole riittäviä uhan torjuntaan. Tästä johtuen päätettiin rakentaa turvavalvomo uuden tuotantolaitoksen yhteyteen, jonne keskitetään koko yrityksen valvonta ja vartioston toiminta. Yrityksen alueella aloitettiin 24/7-perusteinen valvonta ja vastetoiminta.

Valvonnan näkyvyyttä tehostettiin turvaorganisaation läsnäololla sekä toimisto- että tuotantolaitoksilla. Ulkoalueilla näkyvyyttä tehostettiin lisäämällä valvontakierroksia iltaisin ja yöaikaan.

5.2.12 Pitkän aikavälin projekti- ja rahoitussuunnitelman laadinta

Yrityksen johtoryhmä totesi, että turvajärjestelyjen toteuttaminen on kustannuksiltaan niin suuri, että kehittämiskohteita tulee priorisoida ja toteutuksia tulee jakaa useammalle vuodelle. Turvallisuusjohtajalle annettiin tehtäväksi laatia priorisoitu projektisuunnitelma ja kustannusarvio seuraavalle viidelle vuodelle turvajärjestelyjen kehittämiseksi. Kokonaisturvallisuuden ja projektisuunnitelman toteutumista seurattiin yrityksen johtoryhmän kokouksissa.

6 Johtopäätökset

Syvyyssuuntainen puolustus yrityksen henkilöstön, tärkeiden toimintojen ja omaisuuden suojaamiseksi on monitasoinen järjestelmä. Puolustuksen rakentaminen lähtee yrityksen johtamismallista ja turvallisuuspolitiikan määrittämisestä. Turvallisuuspolitiikan mukaisesti ja turvatoiminnot yrityksen johtamisjärjestelmään integroituina luodaan pohja turvallisuuden johtamiselle. Turvallisuuden johtaminen edellyttää kaikkien yrityksen toimintaan liittyviltä tahoilta sitoutumista yrityksen turvallisuuden periaatteisiin ja hyvää turvallisuuskulttuuria. Hyvä turvallisuuskulttuuri luo pohjan jatkuvalle turvallisuuden kehittämiselle ja sinällään vähentää uhkaa aiheuttavien tilanteiden syntymistä.

Jotta ymmärretään, millainen turvajärjestelmästä tulisi muodostua, on kartoitettava, millaisia todellisia ja todennäköisiä uhkia yritys voi kohdata. Jotta voidaan suojautua mahdollisilta uhkilta, tulee määritellä, mitä suojattavia arvoja yrityksellä on ja missä ne sijaitsevat. Uhkien analysointi antaa työkalun ymmärtää paremmin uhkien luonnetta sekä tarvittavia järjestelyjä ja toimenpiteitä, jotka pitää tehdä uhkien hallitsemiseksi. Uhkien perusteella pystytään tunnistamaan riskejä yrityksen turvallisuusjärjestelmässä ja jatkuvan kehittämisen periaatteiden mukaisesti voidaan riskiperusteisesti parantaa yrityksen hallinnollisia, fyysisiä, teknisiä ja operatiivisia kyvykkyyksiä uhkia vastaan.

Hallinnolliset toimet tukevat turvallisuuskulttuurin kehittämistä ja edistävät yrityksen prosessien sekä toimintaohjeistuksen kehittämistä. Hallinnollisilla toimenpiteillä on suuri merkitys toiminnassa esiintyvien poikkeamatilanteiden ennaltaehkäisyyn ja tilanteen palauttamiseen normaalitilaan.

Fyysisen ympäristön turvajärjestelyillä pystytään vaikuttamaan työntekijöiden liikkumiseen ja rajaamaan pääsyä yrityksen tiloihin ja toimintoihin, joissa sijaitsee yrityksen suojattavia arvoja. Fyysinen ympäristö luo myös esteen uhan aiheuttajalle ja hidastaa uhan aiheuttajan mahdollista haitallista tekoa. Uhka ja sen valmistelu voi jäädä huomaamatta, ellei turvallisuustilanteen seuraamiseen käytetä hyväksi valvontatekniikkaa.

Syvyyssuuntainen puolustus perustuu edellä mainittujen asiakokonaisuuksien kombinaationa, jossa suojattavat arvot sijoitetaan usean vyöhykkeen sisälle, joille jokaiselle vyöhykkeelle on määritelty omat hallinnolliset, fyysiset, tekniset ja operatiiviset menettelyt suojattavan arvon suojaamiseksi. Syvyyssuuntaisen puolustuksen periaatteen mukaisesti jokainen vyöhyke suojattavan arvon ympärillä antaa lisäsuojaa suojattavalle arvolle, ja näin vähentää riskiä suojattavan arvon menettämiselle.

Toteutettaessa syvyyssuuntaista puolustusta on mietittävä uhan toteuttamistavan lisäksi uhan aiheuttajaa. Uhan aiheuttaja voi olla kuka tahansa yrityksen toimintaan liittyvä taho. Erityisesti syvyyssuuntaisen puolustuksen suunnittelussa tulee ottaa huomioon sisäiset eli Insider-uhat. Insider-uhka voi muodostua mille tahansa syvyyssuuntaisen puolustuksen vyöhykkeelle, ja sen aiheuttajalla voi olla merkittävät toimivaltuudet eri vyöhykkeillä. Insiderin mahdollisuuden takia ei voida luottaa siihen, että uhan muodostuminen alkaa aina uloimman vyöhykkeen ulkopuolelta. Jos kuitenkin uhka realisoituu huolimatta kaikista suojautumiskeinoista, on oltava menettelyt puuttua uhan aiheuttajan toimintaan, ja mahdollisimman varhaisessa vaiheessa ilmaista uhan aiheuttajalle sen havaitsemisesta, sekä pyrkiä rajoittamaan uhan aiheuttajan toimintaa ja lopulta estää haitallinen toiminta. Mikäli uhka on pystytty toteuttamaan kokonaisuudessaan, tai osittain, on oltava myös menettelyt toiminnan palauttamiseksi normaalitilaan.

Syvyyssuuntainen puolustus mahdollistaa yritykselle vakaamman toimintaympäristön. Turvallisuus ja turvallisuuden vaaliminen muodostuvat kulttuuriksi, joka on istutettu yrityksen toimintarakenteisiin ja päivittäiseen työhön. Kehittämällä jatkuvasti turvajärjestelmää toiminta muuttuu ennaltaehkäisevämmäksi ja vastustuskykyisemmäksi uhille.

Lähteet

[1] Defence in Depth, Protection in Depth and Security in Depth: A Comparative Analysis Towards a Common Usage Language, Edith Cowan University,12-3-2012.

[2] IAEA nuclear security series no. 27-G, Physical protection of nuclear material and nuclear facilities (implementation of INFCIRC/225/revision 5), Implementing guide international atomic energy agency, IAEA, Vienna, 2018.

[3] NIST Special Publication 800-53. Security and Privacy Controls for Information Systems and Organizations, Rev 5, Sep 2020.

[4] IAEA nuclear security series no. 8, Preventive and protective measures against Insider threats, IAEA, Vienna, ISBN 978–92–0–109908–2.

[5] IAEA Nuclear security series no. 10, Implementing guide, IAEA, Development, use and maintenance of the design basis threat, international atomic energy agency, IAEA, Vienna, ISBN 978–92–0–102509–8.

[6] IAEA Nuclear Security Series No. 24-G, Implementing Guide, Risk Informed Approach for Nuclear Security Measures for Nuclear and Other Radioactive Material out of Regulatory Control, IAEA, Vienna, 2015.

[7] IAEA Nuclear security series no. 7, Nuclear security culture, implementing guide, international atomic energy agency, IAEA, Vienna, ISBN 978–92–0–107808–7.

[8] Field Manual No. 3-19.30, Headquarters Department of the Army, Washington, DC, 8 January 2001.